Milton Keynes Education Trust

New Chapter Primary School

Online Safety Policy

Contents

Aims 3

Approach 3

Legislation and guidance 4

Schools and Other Settings: 4

Responsibilities 5

- Governing body 5
- Headteacher and senior management team 5
- The Designated Safeguarding Leads 5
- MK IT department 6
- Computing Lead 6
- Teaching and support staff 6
- Parents and carers 7

Educating pupils about online safety 7

- Using Project EVOLVE 7

Educating parents about online safety 8

Cyber-bullying 8

- Definition 8
- Preventing and addressing cyber-bullying 8

Acceptable use of the internet in school 9

Pupils using mobile devices in school 9

Training 9

Monitoring arrangements 9

Links with other policies 10

Dealing with Online Safety incidents 10

Revision	Date	Author	Comments

Aims

At New Chapter, the safeguarding and promoting the welfare of children includes protecting children from harm that 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.

As a school, we feel strongly that 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, education and support to protect children online.

At New Chapter, our aims are:

1. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
2. Deliver an effective approach to online safety that pprovides children and young people with information and resources to use the internet and other media safely and protect themselves.
3. Equipping professionals and others who work with children with the information and tools to help children and parents/carers to use electronic media safely.
4. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Approach

Addressing the 4 key categories of risk

To support the delivery of our aims, we approach online safety by addressing the following categories of risk:

- **Conduct** – How children behave online can put them at risk of likelihood to cause or receive risks such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Content** – The risk of being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization, extremism, There is further risk of exposure to unreliable and uncreditable content such as fake news.
- **Contact** – The risk of being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Commercialism** – platforms that may have hidden costs for use, inappropriate advertising on websites, phishing and/or financial scam

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

It reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

A comprehensive list of relevant legislation can be found below:

- 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 and Other Settings:

National guidance produced by UK council for Internet Safety (2020) states that children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As a school, we are responsible for teaching children how to be safe when online in a range of contexts.

Responsibilities

Governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is David Hopkins

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- 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.
- Ensuring access to relevant training for all school staff.
- 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

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- 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.

The Designated Safeguarding Leads

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, computing lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

MK IT department

The MK IT department is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Computing Lead

The Computing lead is responsible for:

- 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.

Teaching and support staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Contributing to the development of Online Safety policies.
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policyTaking responsibility for the security of systems and data.
- 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.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents and carers

Parents and carers are expected to:

- 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.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Educating pupils about online safety

Using Project EVOLVE

At New Chapter, we use the online safety toolkit called 'ProjectEVOLVE'. The ProjectEVOLVE toolkit is based on UKCIS framework "Education for a Connected World" (EFACW) that covers knowledge, skills, behaviours and attitudes across eight strands of our online lives from early years right through to eighteen. These outcomes for each strand per year group are mapped carefully to show progression across each school year. The statements included guide educators as to the areas they should be discussing with children as they develop their use of online technology.

By using ProjectEVOLVE, it offers engaging and focussed activities written to engage and inform children and young people around important steps forward in their online journey.

As a school, we carefully choose which strand to teach before every computing lesson using the resources relevant for the children. This covers progression across all strands from Early Years to Year 6 covering:

- Self-image and identity
- Online Relationships
- Online Bullying
- Heath Wellbeing & Lifestyle
- Privacy & Security
- Copyright and Ownership
- Managing Online Information.

Within all year groups, these strands above are split into small, achievable outcomes that progress throughout the years. All lessons are supported with quality resources and vital questions that make the children reflect carefully on their own online safety.

Pupils will be taught about online safety as part of the Nation Curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and newsletter. This policy will also be shared with parents.

Concerns related to online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Computing Lead, headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Children are not permitted to use mobile phones in school. Children who walk to school without an adult are allowed to bring phones into school and store them in the school office during the day.

Training

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every two year by the headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

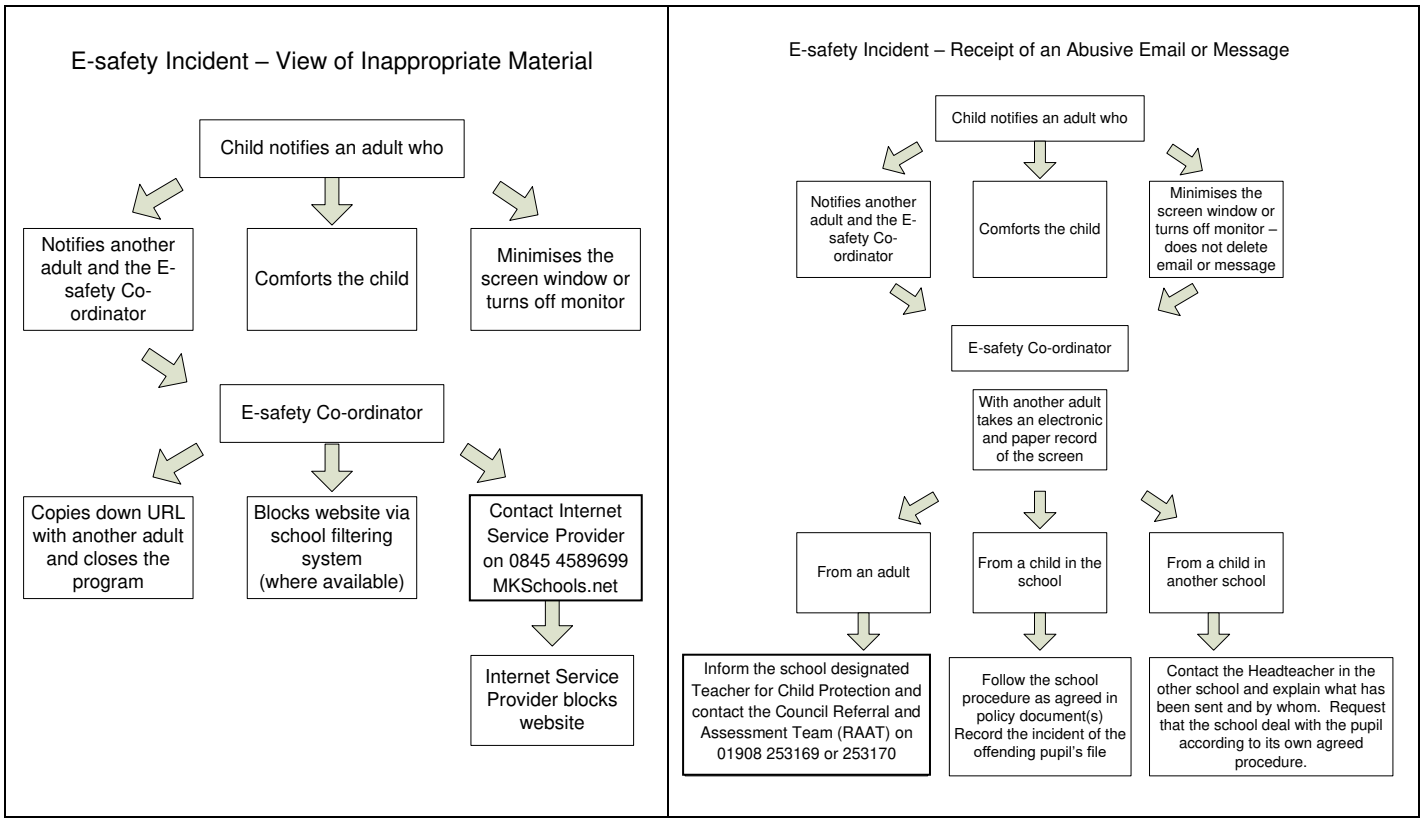
Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Remote Learning policy

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.



If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account

- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.