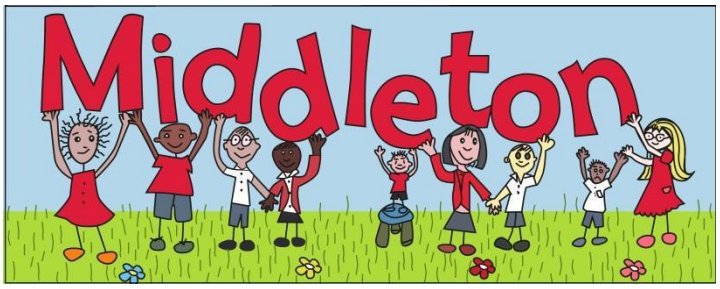


Middleton Primary School eSafety policy

Document Status	
Author	Mr Andy Hudson
Date Written	October 2020 (to address COVID)
Review Requirements	2 Years
Approval Body	Full Governing Body
Date of Approval	
Date next Review	
Publication	Website

At Middleton Primary School, we understand that the virtual world is constantly changing and that we need to be aware of the risks. It is essential that everyone in school uses technology appropriately, safely and legally. We have a responsibility to ensure we teach children the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet or other related technologies.

Purpose of the policy

The internet is becoming as commonplace as TV and telephones and as teachers it is key that we teach children how to safely develop their use of this essential life skill. This document will explain the threats posed by the Internet and its use in a school environment and how teaching staff, pupils and the school body as a whole will minimise these and work safely when using this vital tool.

Core Principles of Internet Safety

· Guided Educational Use – The internet can provide many educational benefits to children including access to information from around the world. Use should be planned, task – orientated and educational within a supervised environment.

· Risk Assessment – Schools need to ensure that they are aware of the risks and pupils and teachers need to know what to do when they come across inappropriate material.

· Regulation – The fact that this resource is ever growing and multi – faceted means its use will undoubtedly attract regulations for its use. The use of some features will be banned, for others fair rules, clearly displayed and explained will help all users make responsible use of this resource.

· Strategies – The document will address these issues and help to ensure that children are safe whilst using the Internet. The key features will be limiting use, supervision and developing the responsibility in children to be vigilant and sensible.

Searching for images safely online

While teachers may find search-engine image searches useful in lesson preparation, they should be used with care and caution in a 'live' classroom setting. At Middleton, we implement the Google SafeSearch technology but staff and children should still be aware of how to deal with inappropriate results if they access them. All search engine requests are monitored and recorded using our monitoring software suite (GoGuardian for Chromebooks and Securus for Windows)

The importance of evaluating and reviewing online resources

Teachers should critically evaluate websites when selecting resources for use in the classroom, and pupils should also be taught these skills as part of their digital literacy skills development.

Safe and effective searching online

Various search tools and techniques can help to locate relevant information quickly, easily and safely online. A good understanding of search tools and techniques will help children to easily find relevant content. The school uses the filtering system provided by E2BN with an additional layer of school based filtering using GoGuardian. This operates at a high security setting to try and ensure that inappropriate website content is blocked.

Minimising 'cyberbullying'

Children will be educated about the potential risks issues from bullying by text message, email or online via websites and social networking sites. This will help to reduce the risks and provide an open culture where bullying of this nature can be freely reported and discussed, whether it takes place in school or elsewhere. The school will deal with cases of cyberbullying in the same way that we would deal with any other cases of bullying. Children are also taught the reporting routes available to them through assemblies and classroom lessons. These sessions detail who the children may want to reports incidents to in school but also the use of the CEOP logo on the school website. This logo links directly to the incident reporting section of the CEOP site.

Mobile technology and e-safety

We do not permit children to bring mobile phones into school. Where it is necessary for them to bring one in, children will need to hand it on arrival. This is because their usage cannot be monitored by staff within school and therefore associated risks (e.g. hurtful texts, inappropriate images, unsuitable internet access) cannot be minimized. Under no circumstances are staff permitted to take photos of children on their own mobile devices (see Use of Images policy).

Email in educational settings

The school provide all staff and Key Stage 2 children with their own school email address. Individual accounts are created as children gain the appropriate skills and knowledge to understand the security implications, and are able to manage their own online communications in a safe and responsible way. The email addresses set up for the children do not allow external access either to or from the account. Children are able to learn how to use email within the safe environment of the school community. The accounts are also monitored and inappropriate language or content is flagged via email to the Esafety coordinator.

Staff email accounts are provided for all staff and may be used for school business. If staff have Webmail accounts (such as hotmail, etc), they should not be used for school business. All school communications should always be sent and managed through a school email account, all staff activity is recorded to minimise safety risks.

Pupils using webmail accounts outside of school should be taught to check for privacy statements when signing up for webmail accounts, not to consent to their details being shared with third parties to minimise the amount of spam they receive, and to make use of any inbuilt filtering tools.

Pupils should be taught appropriate writing and social conventions for using email, including suitable tone and language, so equipping them with the necessary skills to communicate effectively online. Children should also be taught the appropriate behaviours to adopt if they receive an inappropriate or offensive email, such as closing it and seeking advice from a teacher or responsible adult, but never replying to it. This will allow the teacher or responsible adult to check the message, talk through the issues, reassure the pupil that it was not their fault that they received such a message, and take any other action as appropriate.

Embedding e-safety in the primary curriculum

E-safety is embedded within the curriculum as well as being taught discretely - using the Purple Mash Computing scheme. Staff understand the need to work together to ensure that a comprehensive, consistent and continuing programme of e-safety education takes place across subjects, year groups and throughout the school. Children will be taught what to do in the event of accidentally coming across inappropriate material in school. i.e. minimise the screen and go and tell and adult.

During the delivery of esafety lessons that involve children's interactions with others, staff will focus on the 'no blame' approach to addressing the actions of a child. The focus will be on the actions of the perpetrator and not condemning the actions of the victim.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Due to the international scale and linked nature of online content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Unacceptable online behaviour

The school will promote responsible online behaviour for learners. Children and staff will be made aware that the following issues are not acceptable in school:

- finding or guessing someone's password, then using it to gain access to data or services,
- posing as someone else deliberately
- changing or deleting files belonging to others
- deliberately searching for, distributing or downloading unsuitable material

- misuse of school email
- changing computer settings
- deliberately introducing viruses onto the network.

The school will monitor, report and respond to deliberate misuse of computer systems. Users will be made aware that the system monitoring is always active and part of our responsibility to ensure that they are safe. They will also understand that sanctions that will be imposed. Depending on the seriousness of incidents, sanctions might include verbal warnings, temporary IT bans, involvement of parents and carers and general behaviour sanctions in line with the school behaviour policy.

Prevent duty

Middleton Primary is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

We protect children from the risk of radicalisation, for example by using filters on the internet and key logging, to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.

Our Safeguarding, Prevent Duty and eSafety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Dealing with online safety incidents

If children or staff accidentally open unsuitable materials on a school computer the matter should be reported straight to the E-safety co-ordinator. The co-ordinator will review all incidents and decide on an appropriate course of action, applying sanctions with colleagues and informing the Designated Person for Child Protection swiftly as necessary. They will follow the school safeguarding policy, if a child is at any kind of risk, or has suffered harm. Incidents that are at a 'low level' and do not raise an immediate concern will also be reported to the welfare team using the pupil welfare email system so as a longer term picture can be viewed if further incidents occur (see Appendix for Incident flow diagram).

It is becoming increasingly common for social media websites to use interaction metrics, for example hovering over a post, that do not need the user to perform a positive action eg liking a post. These metrics are then used by algorithms to select content that may not be appropriate for children. At Middleton, we use an initial 'no blame' approach when supporting a child that has been exposed to such content.

Creating and maintaining safe websites

The school's website is created by an outside company called E4education. The office staff and the ESafety coordinator are responsible for publishing content to ensure that content is suitable. The Head Teacher reviews changes made by staff frequently. Children will not be named individually on the website and photos or videos will only be put onto the website if parents have signed the relevant consent forms. Parents are asked to complete a form, when the children begin at the school, to give permission for children's images to be used throughout their time at school. Letters that go home to parents will not be published on the site if it provides details of a time and place for a school activity.

Copyright issues for schools and colleges

Under UK law, copyright material published on the internet will generally be protected in the same way as material in other media. Furthermore, each web page may contain several different copyrights if it contains text, music, graphics and so on. Many websites will include a copyright statement setting out exactly the way in which materials on the site may be used. When using websites in educational settings, children should be encouraged to look for copyright information and should be taught that many online resources may have been published illegally without the permission of the copyright owners. This may be particularly the case with media-based content such as music and videos. Any subsequent use of the materials may also be illegal.

Children should be aware that plagiarism (the theft of ideas and works from another author and passing them off as one's own) is not only cheating but, where sufficient is copied, illegal infringement of copyright also constitutes a criminal offence.

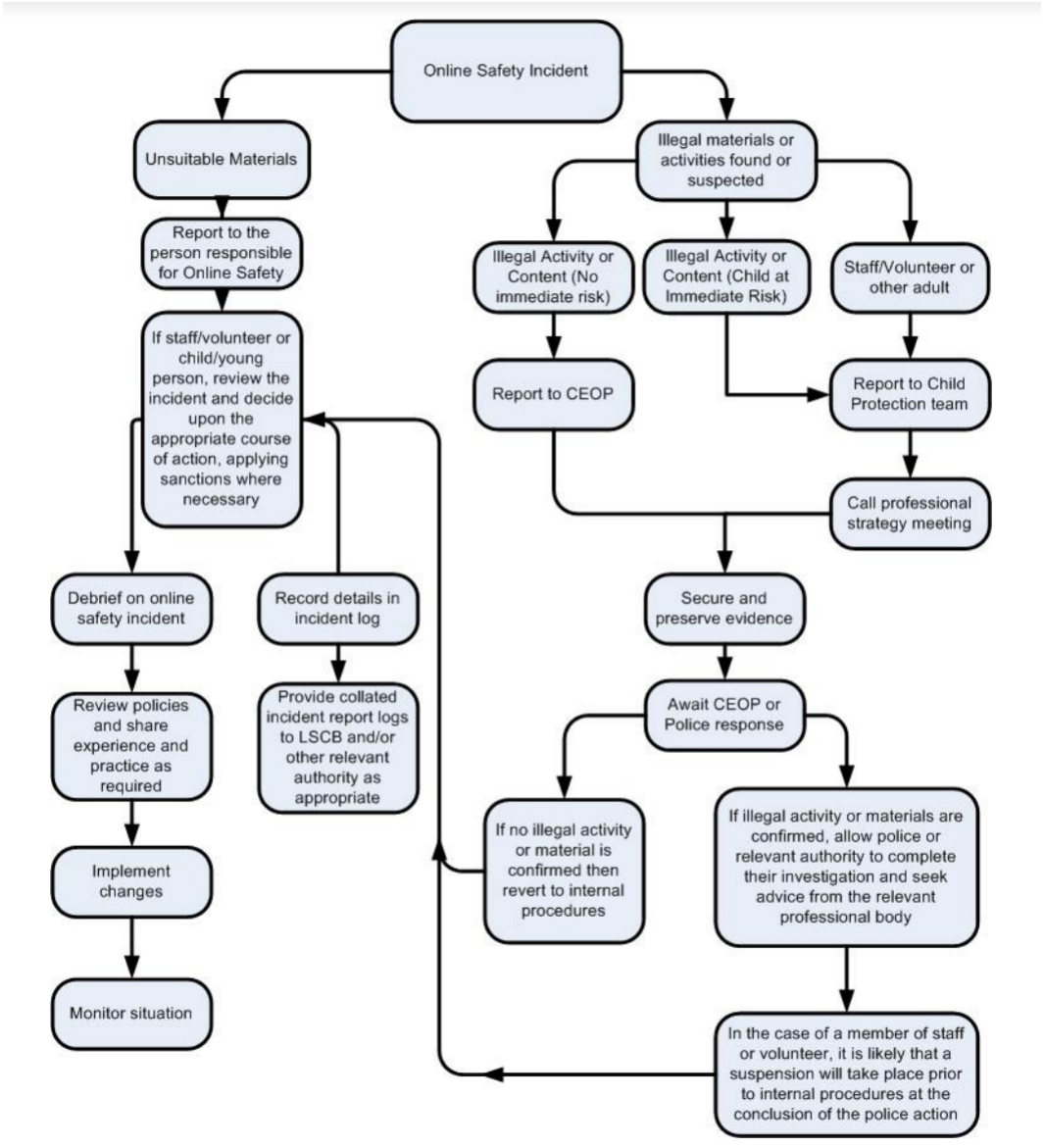
October 2020 update

During the COVID crisis, Middleton is providing laptops for children that are self isolating due to bubble closures. For all Key Stage 2 children, they can only gain access to the internet if they sign in via their school google account. This then allows the school to monitor their web use via the GoGuardian monitoring and filtering system.

We are also providing an esafety newsletter for parents to address current issues regarding the use of technology at home and the actions that they can take to safeguard their children.

Appendix

Incident flow diagram



Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Are responsible for:

- the approval of the E-Safety Policy and for reviewing the effectiveness of the policy

Headteacher and Senior Leaders

Are responsible for:

- ensuring the safety (including e-safety) of members of the school community
- being aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

E-Safety Leader and Subject Coordinator (A.Hudson/M.Smith)

Is responsible for:

- taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- coordinating training and signposts advice for staff
- receiving reports of e-safety incidents and liaising with the SLT and Pupil Welfare team to decide further actions
- reporting regularly to the governing body

Technical staff

Jack Hunt external support services are responsible for:

- ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements in the Local Authority E-Safety Policy and guidance

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they report any suspected misuse or problem to the E-Safety Leader for investigation/action/sanction

Designated team for child protection

Are responsible for ensuring that they have an up to date understanding of the potential for serious child protection issues arising from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying
- promotion of radical / extremist views

Pupils

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Document history

Ver 1.0 - 12th March 2006 – Neil Dixon
Ver 2.0 – 19th October 2008 – Andy Hudson
Ver 3.0 – 18th September 2009 – Andy Hudson
Ver 4.0 – 12th February 2011 – Andy Hudson
Ver 5.0 - 14th February 2013 - Andy Hudson
Ver 6.0 - 20th February 2015 - Andy Hudson
Ver 7.0 – 26th February 2017 – Andy Hudson
Ver8.0 - 12th May 2019 - Andy Hudson
Ver 9.0 - 2nd October 2020 - Andy Hudson