DENHAM VILLAGE SCHOOL

# E-Safety Policy

# E-Safety Policy

Last Updated: 07/20
Update Required: 07/23

| **Creating a Safe ICT Infrastructure in School** |
|---|
| All adults of the school's computer network have clearly defined access rights, enforced using a username/password login system. This helps to protect the network from accidental or malicious attempts to threaten the security of it or the data accessible using it.<br>A permanently-enabled filtering system is provided, which is designed to filter out material found to be inappropriate for use in the education environment. As an additional safety measure, each individual web page is also dynamically scanned for inappropriate content as it is requested, categorised by its content and then access prevented to it if necessary.<br>Access to make changes to overwrite the base-default setting to allow or deny access to a particular website URL can be achieved by contacting the ICT Leader.<br>Security software is installed on all *Windows* machines to prevent any malware (e.g. virus) attacks.<br>Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential. |
| **Rules for Publishing Material Online (inc. Images of Children)** |
| The school's website and VLE are valuable tools for sharing information and promoting children's achievements with a global audience; however, we recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be applied, in accordance with the school's *Child Protection Policy*:<br>• If an image/audio/video recording of a child is used then they should not be named (including in credits).<br>• If a pupil is named, their image/audio/video recording should not be used (no surnames should be published).<br>• Only images of children in suitable dress should be used.<br>• Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.<br>• Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.<br>Comments submitted to posts on the website must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).<br>Children will likely use a variety of online tools for educational purposes during their time at the school. |
| **Children Rules for Acceptable Internet Use** |
| Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes. |
| **Staff/Governor Rules for Acceptable Internet Use** |
| Staff and governors are contractually obliged to use the Internet safely, appropriately and professionally within school, following the same expectations and rules as given to visitors.<br>They are aware that they are role models for others and so should promote and model the high expected |

standards of behaviour at all times.

**E-Safety Education & Training**

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential e-safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

E-Safety education will be provided in the following ways:

E-Safety within the Curriculum

Reception and Key Stage 1 & 2

At this level, use of the Internet will either be quite heavily supervised or based around preselected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them feel uncomfortable.

E-Safety Training for Staff and Governors

The Computing and ICT Leader is a CEOP Ambassador. Staff receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues.

E-Safety Advice for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides advice about how to keep children safe when using the internet to enable them to better understand the issues surrounding new technologies and to help them support their children in developing sensible e-safety behaviour.

**Responding to Unacceptable Internet Use by Children**

Children should be made aware that all e-safety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however staff are trained in how to proceed following a breach using the advice in the school's Child Protection Policy.

**Responding to Unacceptable Internet Use by Staff and Visitors**

Failure to comply with the *Rules for using the Internet safely* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, *Child Protection Policy* and the law. Misuse should be reported without delay.

**Review**

This policy and procedures will be reviewed **annually.**