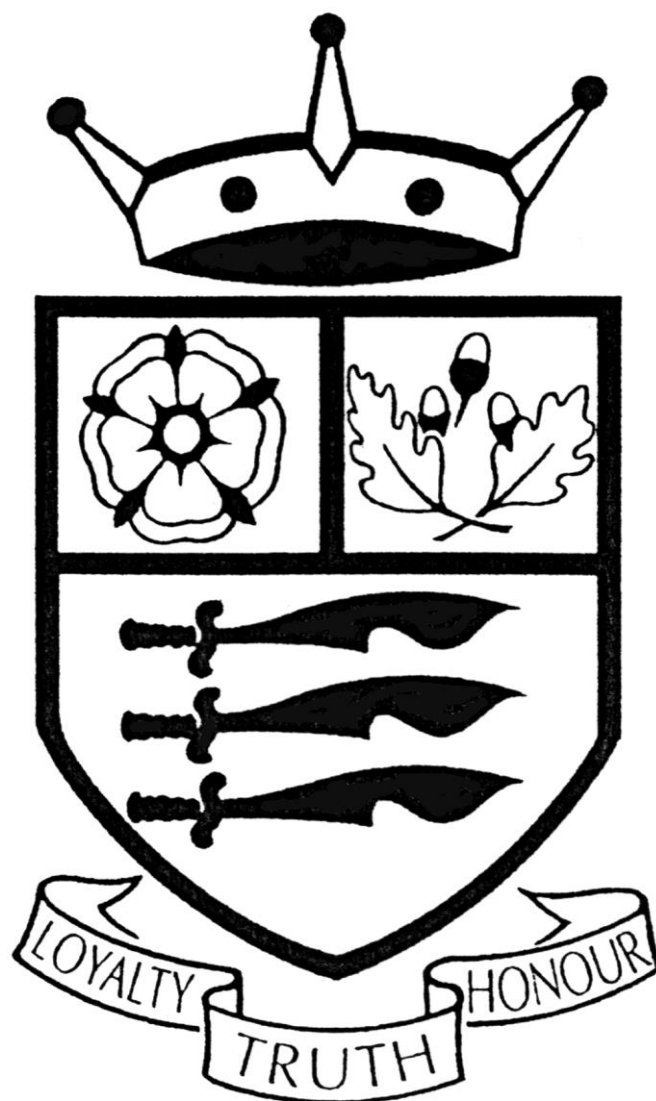


West Lodge Primary School



E-Safety Policy

Rationale

At West Lodge Primary School, we are committed to ensuring the safety of our children and staff at all times. This policy is designed to ensure the online safety of all West Lodge Primary School children and staff in addition to providing help and support to parents and carers. The policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of children 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 published Behaviour Policy. West Lodge Primary School will manage incidents that transgress this policy in conjunction with the school's Positive Behaviour Policy, Safeguarding and Child Protection Policy and Acceptable ICT Use Agreement.

West Lodge Primary School is a Rights Respecting school. The E-Safety Policy is underpinned by the United Nations Convention on the Rights of the Child. (http://www.unicef.org/crc/index_30160.html)

- Article 17: Every child has the right to reliable information from the media. This should be information that children can understand. Governments must protect children from materials that could harm them.
- Article 34: Governments should protect children from all forms of sexual exploitation and abuse. This provision in the Convention is augmented by the Optional Protocol on the sale of children, child prostitution and child pornography.
- Article 36: Children should be protected from any activity that takes advantage of them or could harm their welfare and development

Roles and Responsibilities

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-safety incidents and monitoring reports. The role of the E-Safety Governor will include:

- regular contact with the E-Safety Leader/Computing Leader

- regular monitoring of e-safety incident logs

Headteacher and Senior Leadership Team: The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Leader/Computing Leader. The Senior Leadership Team will receive regular monitoring reports from the E-Safety Leader/Computing Leader

E-Safety Leader / Computing Leader

- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school's E-Safety policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- provides training and advice for staff
- liaises with Harrow Local Authority
- liaises with school technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments
- liaises with Governor responsible for to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

ICT Technician

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- school meets required e-safety technical requirements and any Harrow Local Authority or statutory guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection procedure, in which passwords are regularly changed.
- filtering is applied and updated on a regular basis.
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to E-Safety Leader, Assistant Headteachers, Deputy Headteacher and Headteacher.
- that monitoring software / systems are implemented and updated as agreed in school.

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 have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the Headteacher or E-Safety Coordinator for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- E-Safety procedures are embedded at the beginning of each academic year.
- children understand and follow the E-safety and acceptable use policies.

- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that children know what to do if they encounter something inappropriate.