Oak Lodge Primary School

e-Safety Policy

	Name	Date
Policy written by		
Agreed by committee	PPC Committee	June 2016
Next Review June 2019		

This document is available in alternative formats on request

E-safety Policy

Rationale

> *"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*
>
> *To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."* DfE, eStrategy 2005

The Internet is a fast moving and constantly evolving resource which is a vital tool in providing an interactive and engaging education. As an open environment, the internet also poses risks for all its users. This policy outlines what Oak Lodge staff, governors, parents and pupils do to ensure the safest use of the internet.

Roles and Responsibilities

E-safety Coordinator

The e-safety coordinators oversees all digital safeguarding at Oak Lodge. Key responsibilities include:

- developing an e-safe culture
- being the main point of contact on issues relating to e-safety
- putting together and leading an e-safety team
- raising awareness and understanding of e-safety issues amongst all stakeholders, including parents and carers
- embedding e-safety in staff training, continuing professional development and across the curriculum and learning activities
- keeping a log and reporting on e-safety incidents
- keeping up with relevant e-safety legislation
- liaising with the schools Child Protection Officers
- liaising with the LA, LGfL and other agencies as appropriate
- reviewing and updating the e-safety policy and procedures regularly.

E-safety Coordinators: School Business Manager and ICT Subject Leader

Staff

Members of staff are responsible for:

- familiarising themselves with and following this policy
- signing and following the "Staff Acceptable Use Agreement"
- developing an e-safe culture
- teaching e-safety to pupils

- setting an example for safe use of ICT.

Governors

Governors are responsible for:

- familiarising themselves with and following this policy
- supporting an e-safe culture

ICT Technicians

Oak Lodge's ICT technicians are responsible for:

- keeping the schools network secure
- updating and maintaining the school's security software
- setting permissions and updating network access for different groups of users
- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network

Pupils

Pupils are responsible for:

- following the "Pupil's Acceptable Use Agreement"
- being part of an e-safe culture
- participating in e-safety lessons

Parents/Carers

Parents/Carers are responsible for:

- supporting the school's e-safe culture
- supporting their children with managing e-safety risks at home
- following the "Parents Acceptable Use Agreement"

Education and Communication

The e-safety policy will be reviewed every three years; alongside this, staff and governors will updated and informed of any changes to the policy. This e-safety policy will form part of the school induction pack and will be discussed with new members of staff, governors and teaching students (including work experience placements) when joining the school. Upon joining the school every member of staff, parent and student will be required to sign the appropriate acceptable use agreement.

At the beginning of every academic year each class will be taught e-safety as part of their ICT curriculum.

There will be an annual e-safety update for parents and carers in the school newsletter to ensure that they are aware of the e-safety procedures and any changes or updates to them.

Safe use procedures and practices

Education

Oak Lodge:

- fosters a 'No Blame' environment that encourages children to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- ensures children and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- ensures children and staff know what to do if there is a cyber-bullying incident;
- ensures all children know how to report abuse;
- has a clear, progressive e-safety education programme throughout all Key Stages, built on LA/London/national guidance. Children are taught a range of skills and behaviours appropriate to their age and experience, such as:
  - to STOP and THINK before they CLICK
  - to discriminate between fact, fiction and opinion;
  - to develop a range of strategies to validate and verify information before accepting its accuracy;
  - to skim and scan information;
  - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know some search engines/web sites that are more likely to bring effective results;
  - to know how to narrow down or refine a search;
  - to understand 'Netiquette' behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;
- ensures that when copying materials from the web, staff and children understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;
- ensures that staff and children understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming/gambling;
- ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- makes training available annually to staff on the e-safety education program;

- runs a rolling programme of advice, guidance and training for parents, including: information leaflets; in school newsletters; on the school web site; demonstrations, practical sessions held at school; distribution of 'think u know' for parents materials suggestions for safe Internet use at home; provision of information about national support sites for parents.

Internet

Oak Lodge:

- supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older children have more flexible access;
- we use the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- is vigilant when conducting 'raw' image search with children e.g. Google image search;
- informs users that Internet use is monitored;
- informs staff and students that that they must report any failure of the filtering systems directly to the teacher then the e-safety coordinator. Our systems administrators report to LGfL where necessary;
- blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- only uses approved or checked webcam sites;
- has blocked child access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;
- requires children (and their parent/carer) from Key Stage 1 and 2, to individually sign an acceptable use agreement form which is fully explained and used as part of the teaching programme;
- uses closed/simulated environments for email with Key Stage 2 pupils;
- requires all staff to sign an acceptable use agreement form and keeps a copy on file;
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour policy;
- makes information on reporting offensive materials, abuse/bullying etc available for pupils, staff and parents;
- immediately refers any material we suspect is illegal to the appropriate authorities

Email

Oak Lodge:

- does not publish personal email addresses of children or staff on the school website. We use a group email address admin@oaklodge.bromley.sch.uk;

- if one of our staff or children receives an email that we consider is particularly disturbing or breaks the law we contact the police;
- accounts are managed effectively, with up to date account details of users
- messages relating to or in support of illegal activities may be reported to the authorities;
- spam, phishing and virus attachment can make email dangerous; filtering software is used to stop unsuitable mail, LGfL emails reject 9 out of 10 emails received.

Pupils:

- pupils can only use the VLE email accounts on the school system;
- pupils are introduced to, and use email as part of the ICT scheme of work;
- we use whole-class or group email addresses at Key Stage 2. Exceptions are projects with named schools, and for these we allow the children use of a filtered and carefully monitored email system for the period of the project;
- year 3 children are introduced to principles of email through closed 'simulation' software.
- pupils are taught:
    - about the safety and 'netiquette' of using email i.e. not to give out their email address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
    - that an email is a form of publishing where the message should be clear, short and concise;
    - that they must not reveal private details of themselves or others in email, such as address, telephone number, etc.
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages,
    - not to delete malicious of threatening emails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' email letters is not permitted;
    - pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff:

- staff can only use the LGfL and VLE email accounts on the school system;
- staff use LGfL and VLE email systems for professional purposes;
- access in school to external personal email accounts may be blocked;
- emails sent to external organisations are written carefully in the same way as letters;

- staff sign the appropriate Acceptable Use Agreement to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.
-

Use of Digital Images

At Oak Lodge:

- the Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- uploading of information to the website is restricted to the School Business Manager and the Headteacher;
- the school web site complies with the school's guidelines for publications;
- most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- the point of contact on the web site is the school address and telephone number. Home information or individual email identities will not be published;
- photographs published on the web do not have full names attached;
- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- digital images/video of children are stored on the secured school network ;
- we do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- we do not include the full names of children in the credits of any published school produced digital materials/DVDs;
- staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- pupils are only able to publish to their own 'safe' VLE area;
- pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their curriculum;
- pupils are taught about how images can be abused in their e-safety education programme.

Network, Equipment and Data

Oak Lodge:

- ensures staff read and sign that they have understood the school's Acceptable User Agreement. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- makes it clear that staff must keep their log-on username and password private and must not leave them where others can find (staff are prompted to change their passwords every 30 days);
- makes clear that children should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- has set-up the network with a shared work area for children and one for staff. Staff and children are shown how to save work and access work from these areas;

- requires teachers to always log off when they have finished working or lock the computer when they are leaving the computer unattended;
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- requests that teachers and children do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- has set-up the network so that users cannot download executable files/programmes;
- has blocked access to music download or shopping sites - except those approved for educational purposes;
- scans all mobile equipment with anti-virus/spyware before it is connected to the network;
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by ICT technicians or Site Manager. Any ICT equipment installed is checked by our ICT technicians;
- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- provides children and staff with access to content and resources through the approved VLE which staff and children access using their shibboleth compliant username and password;
- uses the DfE secure access website for all CTF files sent to other schools;
- ensures that all child level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- reviews the school ICT systems regularly with regard to security.

Date Policy Approved: June 2016
Policy to be Reviewed: June 2019