Gresham Primary School

E-safety Policy

What is E-Safety?

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. Access to this kind of information is better regulated through other communications media. As a result of the interactivity of new technologies, publishing personal information on the internet can compromise personal security and that of others. It is illegal to store images showing child abuse and to use e-mail, text or Instant Messaging to 'groom' children but, unfortunately, these things do still happen.

E-Safety covers issues relating to children, young people and adults when using the Internet, mobile phones and other electronic communications technologies, both in and out of school.

E-Safety provides education on risks and responsibilities of using technology and is part of the 'duty of care' which applies to everyone working with children. It is also about making sure that the school provides safeguards and raises awareness to enable users to control their own online experiences.

Technical and Infrastructure approaches

a) Access and security

This school:

- Has an educational filtered secure broadband connection provided through the London Grid for Learning (LGfL);
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and management of filters is only available to staff with the approved 'web filtering management' status;
- Filters access to some YouTube videos
- Uses user-level filtering where relevant, thereby blocking or opening up websites appropriate to the age / stage of the students;
- Ensures the network is healthy through use of anti-virus software and computers are updated regularly;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal data;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where appropriate;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems are robust and protect students as effectively as possible;
- Ensures that Systems Administrators keep up-to-date with LGfL services and policies;
- Uses Google Classroom for setting weekly home learning (and, in the event of school closure, online learning) for which all children/staff have a username and password to access.

b) Passwords

This school:

- Uses individual named system log-ins for all staff and Year 2 to Year 6 users for computer systems and Google Classroom.
- Makes it clear that staff and pupils must keep their passwords private, must not share them with others and must not leave them where others can find them.
- Staff are required to keep pupils' logins secure.

c) Email

This school:

- Provides staff with an email account for their professional use and makes clear their personal email should be through a separate account;
- Does not publish personal email addresses of pupils or staff on the school website. We use a school office email address for communications with the wider public. Year group emails are currently available for direct communication with class teachers.

Policy and procedures:

This school:

- Is vigilant in its supervision of pupils' use of technology, as far as is reasonably possible. We use common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff have signed an acceptable use agreement form and understand that they must proactively report any e-safety concerns.
- Requires staff to preview websites before use to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids
- 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*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Requires parents to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;

- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;
- 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 management system;
- Ensures the named child protection officer has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides Esafety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

a) Pupils e-safety curriculum

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the website to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - SMART rules of e-safety
    - 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 how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - 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, location, 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;
- [for older pupils] to understand why and how some people will use a false identity and/or may deceive others that they talk to online.

b) Staff

This school:

- Ensures that when copying materials from the web, staff and pupils 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 pupils 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 send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes training available annually to staff on the e-safety education program;

c) Parents

This school:

- 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.

Social Networking:

- Teachers are not allowed to run social network spaces for pupils use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communication.
- The school does not permit pupils to access any social networking sites while at school.
- The school strongly recommends that pupils do not have their own Facebook (and similar) accounts, since such accounts should not be created by persons under the age of 13.
- The school recommends that parents carefully monitor their child's access to and use of social networking sites outside of school.
- School staff are required to ensure that in their personal use of technology outside school that:
  1. No reference should be made in social media to pupils, parents/carers or school staff;
  2. They do not engage in online discussion on personal matters relating to members of the school community;
  3. They do not engage in online discussion on school policy and matters related to school, nor do they reveal sensitive or confidential information about staff or pupils;
  4. Security settings on personal social media profiles should be checked.
  5. Any breach of privacy as described above may result in disciplinary action.

Monitoring :

The School reserves the right to monitor staff communications in order to:

- establish the existence of facts
- ascertain compliance with regulatory or self-regulatory procedures
- monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes
- prevent or detect crime
- investigate or detect unauthorised use of the School's telecommunication system
- ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations
- gain access to routine business communications for instance checking voice mail and e-mail when staff are on holiday or on sick leave.

Confirmation the E-Safety in respect of Gresham Primary School has been discussed by the Governing Body:

Signed by:

Chair of Governors: …… Date: ……

Head Teacher: …… …… Date: ……

Agreed at the Governing Body Meeting on: ……

Minute Reference: ……