Princes Avenue,
Kingsbury, London,
NW9 9JL

Telephone: 020 8204 3531
Email: admin@rgreeninf.brent.sch.uk
www.rgreeninf.brent.sch.uk

Managing the Internet Safely

Technical and Infrastructure approaches

Roe Green Infant school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects

  to the 'private' National Education Network;

- 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 is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and

  network set-up so staff and pupils cannot download executable files;

- Uses individual, audited log-ins for all staff users;
- 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 were staff need to access personal level data off-site;

- 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;

- Provides highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1

  pupils; Uses Londonmail with students as this has email content control and the address does not identify the student or school;

- Provides staff with an email account for their professional use, London Staffmail / LA email and makes clear personal email should be through a separate account;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users /setting-up applications and Internet web sites, in the ICT suite;
- Has additional local network auditing software installed;
- Works in partnership with the LGfL to ensure any concerns about the system are

  communicated so that systems remain robust and protect students;

- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and Ensures the Systems Administrator / network manager is up-to-date with LGfL services and

policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies.

Legal framework

- This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on: https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet
    - online abuse
    - bullying
    - child protection.
- We believe that….
    - children and young people should never experience abuse of any kind
    - children should be able to use the internet for education and personal
- development, but safeguards need to be in place to ensure they are kept safe
- At Roe Green Infant school, we are vigilant in its supervision of pupils' use of internet at all times, as far as is reasonable, and 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 understands that they
- must report any concerns;
- Ensures pupils only publish within the appropriately secure school's learning environment, such as the London MLE.
- https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way 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. Our organisation is held securely and shared only as appropriate.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos 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. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;

- Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
- 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 in this instance it is Marina Aziz (DSL), has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Provides E-safety advice for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

We will seek to keep children and young people safe by:

• Refer all online referrals to Marina Aziz (online safety coordinator)
• providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
• supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
• supporting and encouraging parents and carers to do what they can to keep their children safe online
• developing an online safety agreement for use with young people and their parents or carers
• developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
• reviewing and updating the security of our information systems regularly
• ensuring that user names, logins, email accounts and passwords are used effectively
• ensuring personal information about the adults and children who are involved in ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
• providing supervision, support and training for staff and volunteers about online Safety.
• examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

• having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
• providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
• making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
• reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

• child protection
• procedures for responding to concerns about a child or young person's wellbeing
• dealing with allegations of abuse made against a child or young person
• managing allegations against staff and volunteers
• code of conduct for staff and volunteers
• anti-bullying policy and procedures
• photography and image sharing guidance.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

• child protection
• procedures for responding to concerns about a child or young person's wellbeing
• dealing with allegations of abuse made against a child or young person
• managing allegations against staff and volunteers
• code of conduct for staff and volunteers
• anti-bullying policy and procedures
• photography and image sharing guidance

Education and training:

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 URL 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: o to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion; o to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information; o 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; o
- 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; o
- 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; o
- to understand why they must not post pictures or videos of others without their permission; o to know not to download any files – such as music files - without permission; o
- to have strategies for dealing with receipt of inappropriate materials; o [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons; or Extremism
- 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;
- 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.

Roles	**Responsibilities**
Headteacher	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security(SIRO)

	• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and • support staff who carry out internal Online safety procedures(e.g. network manager)
Online Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents • promotes an awareness and commitment to Online safeguarding throughout the school community • ensures that Online safety education is embedded across the curriculum • liaises with school Computing technical staff • To communicate regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident • To ensure that an Online safety incident log is kept up to date • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • Online bullying and use of social media
Governors / Online safety governor	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the

	Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include: • • regular review with the Online Safety Co-ordinator / Officer (including Online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly
Network Manager/technician	• To report any online safety related issues that arise, to the Online safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school IT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid. • that he / she keeps up to date with the school's Online safety • policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • that the use of the network / Virtual Learning Environment • (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems.
- Staff are responsible for keeping their password private.
- We require staff to use **STRONG passwords for access in to our MIS systems**
- **We require staff to change their passwords into the MIS, LGfL USO admin site every 90 days /twice a year.**

……Designation……..Date…….. Signed
……Designation……..Date…….. Signed

Reviewed:	14/11/22	Action:	
Reviewed;		Action:	
Reviewed;		Action:	

Reviewed and changes made Jan 23