KEW RIVERSIDE PRIMARY SCHOOL

Kew Riverside Primary School E-Safety Policy Incorporating Acceptable Use, Bring your own Devices and Cookies Policies

Committee ownership for this policy	Curriculum and Achievement Committee
Must be approved by FGB:	Full governing body or proprietor
Required by: 1 / 2 • Where 1 is indicated, the requirement is statutory • Where 2 is indicated, the requirement is recommended	2
Frequency of review:	Annually
Date last reviewed:	November 2018
Date of next review:	November 2019
Display on website:	Yes
Purpose:	To support all stakeholders in understanding why positive behaviours are valued and how we manage behaviour which falls short of the standards we expect. The policy also outlines how we communicate with parents and other stakeholders.
Consultation:	Staff and Governors
Links with other policies:	Safeguarding and Child Protection Policy

1. Introduction and Overview

This policy applies to all members of Kew Riverside Primary School community (including staff, pupils / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / ICT systems, both in and out of Kew Riverside Primary School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the Kew Riverside Primary 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 / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Kew Riverside Primary School with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of Kew Riverside Primary School
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse such as cyber-bullying which are cross-referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- So-called 'lifestyle' websites, for example pro-anorexia/self-harm/suicide sites
- 'Hate' sites

- Content validation: how to check authenticity and accuracy of online content
- Contact
- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
- Conduct

Privacy issues, including disclosure of personal information

- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

Responsibilities:

Headteacher

- To take overall responsibility for:
    - e-Safety provision
    - data and data security (SIRO – Senior Information Risk Owner)
- 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 e-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 provide regular monitoring reports
- To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager)

E-Safety Co-ordinator / Designated Child Protection Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Ensures that e-safety education is embedded across the curriculum
- Liaises with school ICT technical staff
- To communicate regularly with SLT and the designated e-Safety Governor 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 e-Safety incident
- To ensure that an e-Safety /Behaviour/Serious 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
    - Cyber-bullying and use of social media
- Educating Parents and raising awareness as instructed by Head

Governors / E-safety governor

- To ensure that the school follows all current e-Safety advice to keep the children and staff safe
- To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities
- The role of the E-Safety Governor will include:
    - Regular review with the E-Safety Co-ordinator / Officer (including E-safety incident logs, filtering / change control logs)

Computing Curriculum Leader

- To oversee the delivery of the e-safety element of the Computing curriculum
- To liaise with the e-safety coordinator regularly

Network Manager/technician (We Support IT Solutions Limited)

- To report any e-Safety related issues that arises, to the e-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 ICT system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- 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 e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-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 e-security and technical procedures.

Data Protection Officer
- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

LGfL Nominated contact(s)
- To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts

Teachers
- To embed e-safety issues in all aspects of the curriculum and other school activities
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant)
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

All staff
- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement
- To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- To report any suspected misuse or problem to the e-Safety coordinator
- To maintain an awareness of current e-Safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils
- Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (NB. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (especially for project work)
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.

- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To help the school in the creation/ review of e-safety policies

Parents/carers

- To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To access the school website / pupil records in accordance with the relevant school Acceptable Use Agreement
- To consult with the school if they have any concerns about their children's use of technology

External groups

- Any external individual / organisation will sign an Acceptable Use Agreement prior to using any equipment or the internet within school

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staffroom/planning folders
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];

    - Referral to LA / Police.
- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyber-bullying are dealt with in accordance with our Behaviour & Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the Leadership Team and approved by Governors and other stakeholders such as the PTA. All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL e-Safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK;
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - 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 acceptable 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;
- To understand the impact of cyber-bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber-bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through the end-user Acceptable Use Agreement which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- 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 respect and acknowledge 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;

Staff and governor training

This school

- 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 regular training available to staff on e-safety issues and the school's e-safety education program;<annual updates/ termly staff meetings etc>.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safeguarding policy and the school's Acceptable Use Agreement.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreement to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

This advice is delivered by the LA advisor on ICT.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management
In this school:
- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering
This school:
- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper 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;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils;
- 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;
- ses 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;

- 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;
- 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;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's website a key way to direct pupils 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; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- 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;
- Provides advice and 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 – Police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the London USO system;

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- *Has additional local network auditing software installed;*
- Ensures the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all data internally and externally conforms to the UK data protection requirements.
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the General Data Protection Regulations 2018 where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password and user account for data security purposes;
- We provide pupils with a year group network log-in username (and password from Year 2).
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform *and (for older pupils) their own school approved email account*;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as 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 pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or 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. [Users needing access to secure data are timed out after 10 mins and have to re-enter their username and password to re-enter the network.];
- Requests that teachers and pupils 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 and we also automatically switch off all computers at 6.30 p.m. to save energy;

- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites via Atomwide firewall – 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.
- *Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;*
  e.g. Borough email or Intranet; finance system, Personnel system etc
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- 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;
  e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- 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;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child; Assessment Tracker (Pupil Asset)
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords

- 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.
- 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 into our MIS system>.
- We require staff to change their passwords into the MIS, LGfL USO admin site, <other secure system> <every 90 days / twice a year>.

E-mail

This 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;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with pupils as this has email content control
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help

protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Year R/1 pupils are introduced to principles of e-mail through closed 'simulation' software.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail 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 e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

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

Staff:

- Staff can only use the LA or LGfL e mail systems in school. Other systems such as Hotmail or email can only be used on staff's personal devices.
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX*, named LA system;*
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper:
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: <e.g. X administration officer >
- The school web site complies with the statutory DfE 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, telephone number and we use a general email contact address, e.g. info@kewriverside.richmond.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

- Uploading of information on the schools' website is shared between different staff members according to their responsibilities

Social networking

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

- **School staff will ensure that in private use:**
    - No reference should be made in social media to pupils / pupils, parents / carers or school staff
    - They do not engage in online discussion on personal matters relating to members of the school community
    - Personal opinions should not be attributed to the *school* or local authority
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- **Video Conferencing**
  This school
    - Only uses the LGfL / Janet supported services for video conferencing activity and gotomeetings.com
    - Only uses approved or checked webcam sites;
- **CCTV**
    - We have CCTV in the school as part of our site surveillance. We will not reveal any recordings unless a formal request to the Designated to Control Access (the images are *retained by the Support Provider for 30 days*), without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record on spreadsheet.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
- staff,
- governors,
- pupils
- parents

    - This makes clear all staff responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have <secure area(s) on the network to store sensitive documents or photographs>.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after <10 mins idle time>.
- We use <encrypted flash drives> if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use < RAv3 / VPN solution> for remote access into our systems.
- We use <LGfL's USO FX> to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in <lockable storage cabinets in a lockable storage area>.
- All servers are <in lockable locations and> managed by DBS-checked staff.

- We <lock any back-up tapes in a secure, fire-proof cabinet>. <Back-ups are encrypted>. <No back-up tapes leave the site on mobile devices.>
- We use < LGfL's GridStore remote secure back-up / named alternative solution> for disaster recovery on our <network / admin, curriculum server(s)>.
- We comply with <the WEEE directive on equipment disposal> by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and <get a certificate of secure deletion for any server that once contained personal data>.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, <is disposed of through the same procedure>.
- Paper based sensitive information is <shredded, using cross cut shredder / collected by secure data disposal service>.
- <We are using secure file deletion software>.

Equipment and Digital Content

Bring Your Own Devices

The School recognises that mobile technology offers valuable benefits to staff including from a teaching and learning perspective and to visitors. Our School embraces this technology but requires that it is used in an acceptable and responsible way.

Personal mobile phones and mobile devices

- Designated 'mobile use free' areas are situated in the setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - changing areas.
- Visitors (including parents), staff and children may not use their own mobile phones, devices or cameras to take photographs within our **Early Years Foundation Stage**.
- Mobile phones brought into school are entirely at the staff member, pupils' & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils' mobile phones which are brought into school must be turned off (not placed on silent) and stored in a locked box in the headteacher's office. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny

and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring. Also refer to the Safeguarding and Child Protection Policy before checking mobile devices.
- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings must not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving pupils other than their own children in photographs, video, or audio, and other visitors and staff should not comment in a manner that may cause offence or upset.
- No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school.

Pupils' use of personal devices

- The School strongly advises that a child's mobile phone should not be brought into school.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Children found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will use a school phone where contact with pupils, parents or carers is required, unless they are away from the school building and with the permission of the headteacher.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by a member of leadership.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose. If a work-provided device is unavailable, a personal device may be used ONLY with the permission of the headteacher.
- If a member of staff breaches the school's policy then disciplinary action may be taken.

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

- 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;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Access to the School's internet connection

The School provides a wireless network that staff and visitors to the School may use to connect their mobile devices to the internet. Access to the wireless network is

At the discretion of the School, and the School may withdraw access from anyone it considers is using the network inappropriately.

The School cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The School is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the School's wireless network. This activity is undertaken at the owner's own risk and is discouraged by the School. The School will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the School's wireless network.

Access to School IT services

School staff are permitted to connect to or access the following school IT services from their mobile devices:

The school e-mail system;

The school calendar system

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an e-mail attachment). Staff shall delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information accessed through these

services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported to the School as soon as possible.

Staff must not send school information to their personal e-mail accounts.

If in any doubt, a device-user should seek clarification and permission from the School's network manager before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

Monitoring the use of mobile devices

The information that the School may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school IT services or the School internet connection should report this to the School as soon as possible.

Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the School's E-safety, Staff behaviour and Staff code of conduct for use of the computer network and the internet policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

Compliance with Data Protection policy

Staff compliance with this E-Safety Policy is an important part of the School's compliance with the General Data Protection Regulation 2018 / Data Protection Act 1998. Staff must apply this policy consistently with the School's Data Protection policies.

Support

The School takes no responsibility for supporting staff's own devices; nor has the School a responsibility for conducting annual PAT testing of personally-owned devices.

Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the School to risks. If a breach of this policy occurs, the School will respond immediately by issuing a verbal, then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the School will permanently withdraw permission to use user-owned devices in school.

Incidents and response

The School takes any security incident involving a staff member's or visitors personal device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to the school office in the first instance. Data protection incidents should be reported immediately to the School's data protection controller.

COOKIES

A cookie, also known as a browser cookie or web cookie, is usually a small piece of data sent from a website and stored in a user's Web Browser.

While a user is browsing a website. They are used by us to help our users navigate the Kew Riverside Primary School website efficiently and perform certain functions. Due to their core role of enhancing or enabling usability or site processes, disabling cookies may prevent users from using certain parts of this website. You can find more information about 'cookies' at: www.allaboutcookies.org

HOW WE USE COOKIES

The Kew Riverside Primary School website uses Google Analytics, a service offered that generates detailed statistics about the visitors to a website. It is the most widely used website statistics service, currently in use on around 55% of the 10,000 most popular websites.

To gather statistical information, Google Analytics use 'performance cookies'. These cookies collect anonymous information about how visitors use websites, for instance which pages visitors go to most often, whether they have been to the site before and how long they remain on each page.

These cookies do not collect personal data. The information these cookies collect is aggregated and therefore anonymous and only used to improve

how a website works. You can find further information on cookies used by Google Analytics at:

https://developers.google.com/analytics/resources/concepts/gaConcepts Cookies

DISABLING COOKIES

Most browsers allow you to reject all cookies, whilst some browsers allow you to reject just third party cookies. For example, in Internet Explorer you can refuse all cookies by clicking Tools, Internet Options, Privacy, and selecting Block all cookies using the sliding selector. Blocking all cookies will, however, have a negative impact upon the usability of many websites, including this one.

KEW RIVERSIDE PRIMARY SCHOOL

Acceptable Use Agreement

Please read through this agreement with your parents and together sign the bottom.

1. You must obtain the permission of your parent(s)/guardian(s) before you can be allowed to use the Internet at school.

2. You must only access those services you have been given permission to use. Search Engines are only to be used with the permission of your parents/guardians.

3. In school, you must not access the service without the permission of a teacher or teaching assistant.

4. The work/activity on the Internet must be directly linked to your school work. Private use of the Internet in school is strictly forbidden.

5. Keep your own passwords or login details a secret. The only people who should know these are you and your parents/guardians.

7. Do not give your own or other peoples personal addresses, telephone, mobile phone numbers to strangers.

8. Use of names of pupils, or photographs of pupils will require written permission from parent(s)/guardian(s). This is recorded on the Parental Permission Form

8. Do not download, use or upload any material and use material which is copyright. Check with a teacher or parent/guardian if you are unsure.

9. Always seek permission from the owner, before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material

10. Under no circumstances should you view, upload or download and material which is likely to be unsuitable for children or schools. This applies to any material of a violent, dangerous, racist, or inappropriate sexual content. If you are not sure about this, or any materials, you must ask your teacher, parent or guardian.

11. Do not upload video or still images of school events (such as Sports Day, Assemblies, School Plays, etc) onto shared media sites such as YouTube. These may show children for whose image you do not have permission to use. Video and stills are for your personal use only.

12. Always respect the privacy of files of other users. Do not enter the file areas of other pupils or staff without obtaining permission from them first.

13. You must agree for the technician, subject leader, teacher or headteacher to view any material you store on the school's computers, or on disks you use on school's computers.

14. The use of strong language, cyber-bullying, swearing or aggressive behaviour is forbidden.

Failure to comply with these rules will result in a letter informing your parents of the nature and breach of rules and appropriate sanctions and restrictions placed on access to school facilities to be decided by the Headteacher.

If you do not understand any part of this Acceptable Use Agreement, you must ask your class teacher, the subject co-ordinator or Headteacher.

Please return this form to the school office. Failure to do so may result in restricted use of school Internet facilities.

We agree with the terms of this acceptable use policy.

Child_____ Child _____ Child _____

Child_____

Parent/Guardian_____ Date_____