KEW RIVERSIDE
20 02
PRIMARY SCHOOL

Online Safety Policy

Committee ownership for this policy	Curriculum and Achievement Committee
Must be approved by FGB:	Full governing body or proprietor
Required by: 1 / 2 • 1 – the requirement is statutory • 2 – the requirement is recommended	2
Frequency of review:	Annually
Date last reviewed:	December 2020
Date of next review:	December 2021
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 Pupil and Staff Online and ICT Acceptable Use Agreements Google Meet Acceptable Use Agreements Twitter policy

Introduction

This policy is part of the School's Statutory Safeguarding Policy and Staff Code of Conduct. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Leadership team and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Contents Page

1. Introduction and Overview

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 IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying referring also to our Behaviour Policy and Safeguarding and Child Protection Policy
- 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Sexting
- Social or commercial identity theft, including passwords

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

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

Roles and responsibilities

Role	Key Responsibilities
Headteacher: Liz Strong Senior Leaders: Ardeep Virdi, Rachel Chambers and Emily Spencer Data Protection Officer (DPO): Peter Cowley	• To be trained up to Level 3 Safeguarding • To take overall responsibility for online safety provision • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure annual radicalisation updates and suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Data Protection Officer (DPO) • 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 • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Designated Safeguarding Lead (DSL) DSL: Liz Strong Deputy DSL: Rachel Chambers and Laura Wrigglesworth	• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • 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 online safety incidents are logged as a safeguarding incident • Facilitate training and update annual regarding Safeguarding advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues

Role	Key Responsibilities
	• Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns
Safeguarding Governors (including online safety): Denise Long Peter King Patrick Neave	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the Designated Safeguarding Lead
Computing Curriculum Leader: Will Reber	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician: Trusol overseen by Anna-Marie O'Connor	• To report online safety related issues that come to their attention, to the Designated Safeguarding Lead, Computing Lead and where appropriate the Data Protection Office • To manage the school's computer systems, ensuring - school password policy is strictly adhered to • To ensure systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) through Sophos and LGFL - access controls/encryption exist to protect personal and sensitive information held on school-owned devices (Bitlocker) • To ensure the school's policy on web filtering is applied and updated on a regular basis • That they keep 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 school technology and online platforms are monitored weekly through LGFL reports and that any misuse/attempted misuse is reported to the Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
LGfL Nominated contact(s): ?	• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• To embed online safety in the curriculum

Role	Key Responsibilities
	• 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, volunteers and contractors (where appropriate)	• To read, understand, sign and adhere to the school staff Acceptable Online and ICT Use Agreement/Policy, and understand any updates annually. This is signed by new staff on induction • To report any suspected misuse or problem to the appropriate person • To maintain an awareness of current safeguarding and online safety issues and guidance, e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset
Pupils	• Read, understand, sign and adhere to the Pupil Online and ICT Acceptable Use Policy annually • 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 understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Online and ICT Use Agreement with their child/ren. • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety and endorse the Acceptable Use Agreement which includes the

Role	Key Responsibilities
	pupils' use of the Internet and the school's use of photographic and video images
Data Protection Officer: Peter Cowley	• To advise and inform the school and its staff about their obligations to comply with GDPR and any other data protection legislation • To monitor the school's compliance with GDPR, train staff, conduct audits etc. • To be the first point of contact with the ICO and data subjects

Communication

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

- Policy to be published on the school website
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to staff and pupils on entry to the school.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Designated Safeguarding Lead via CPOMs.
- Any concern about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the complainant is referred to the Chair of Governors and the DSG (Designated Safeguarding Governor).

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing, PSHE and RSE curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online 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 pupil Acceptable Use Agreement(s);

- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- 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 Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- Runs a rolling programme of online safety advice, guidance and training for parents

3. Expected Conduct and Incident management

Expected Conduct

In this school:

All users

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should know and understand what the school's rules of appropriate use for the whole school community are

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy;
- all members of the school 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 (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- uses the LGfL age-appropriate filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2 secure file/email to send 'protect- level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect pupils

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users - the LGfL 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;
- 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;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive 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 online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- All pupils have their own unique username and password which gives them access to the Internet and other services; they each have a Google login and a LGFL login.
- 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;
- Requires all users to log off or lock their screen when they have finished working or are leaving the computer unattended as per GDPR school procedures.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- 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;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data in The Cloud;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- To transfer SEND files, for example reports and referral forms which include personal data, secure sending platforms such as Egress, USO-FX or Cisco are used;
- 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);

- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- Staff passwords are to be changed every 90 days.
- We require primary contacts to change their passwords into the MIS, LGfL USO admin site, every 90 days.
- We require staff using critical systems to use two factor authentication.

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;
- 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.
- 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
- 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.

Staff:

- Staff can only use the LA or LGfL e-mail systems on the school system
- Staff will use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- 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);

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;

- 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;
- 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;

Cloud Environments

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social Networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- 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.
- For the use of any school approved social networking will adhere to our Twitter Policy and Staff Code of Conduct.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- 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 and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Where appropriate pupils are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our Pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through the Pupil Acceptable Use Agreement (which they are required to read and follow) and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people. This information is always shared at the start of any parent attended assembly or event.

CCTV:

- We have CCTV in the school as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access, data transfer and asset disposal

At this school:

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff have had a satisfactory DBS check and records are held in single central record (Cpoms Staffsafe)
- Staff have secure areas on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer.
- We use the LGfL USO Auto Update, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Where any protected or restricted data has been held, we get a certificate of secure deletion for any server that once contained personal data.
- We use secure file deletion software when required.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices or hand held device.
- No pupils unless Year 5 and Year 6 should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be kept in the Headteacher’s office and returned at the end of the day.

- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off as per the Acceptable Use agreement.
- No images or videos should be taken on mobile devices apart from the Head teacher's mobile phone or another Senior Leader who is responsible for updating school social media.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring e.g. the mobile telephones of the Head Teacher and Site Manager will be inspected randomly as part of a programme of 'spot checks' to ensure they are used appropriately.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Staff may use their phones during break times and in the staff room. 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.

Storage, Synching and Access

The device is accessed with a school owned account:

- The device (iPADS and laptops) has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be logged and log sent to network manager

The device is accessed with a personal account:

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff will be issued with a school phone where contact with-parents or carers is required, for instance for offsite activities.
- Mobile Phones and personally-owned devices will be switched off. 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 senior leadership team in emergency circumstances.

- 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.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and then report the incident to the Headteacher and DPO.
- If a member of staff breaches the school policy then disciplinary action may be taken.

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 (or annually);
- 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;
- Since the implementation of GDPR 2018, the school has chosen not to act retrospectively. From this point forward the school will obtain permission for the use of images to remain on the school website and other media outlets including social media for a period of 5 years
- Pupils are taught about how images can be manipulated in their online 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 computing 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 identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.