KEW COLLEGE PREP

Internet and On-Line Safety Policy

This policy applies to the whole school including EYFS

This policy is written with due regard to the following:
Keeping Children Safe in Education (KCSIE) (Sept 2022)
Working Together to Safeguard Children (Sept 2018)
ISI Handbook for the Inspection of Schools: Commentary on the Regulatory Requirements (Sept 2019)
The Prevent Duty: Departmental Advice for schools and childminders (June 2015)
Revised Prevent Duty guidance: for England and Wales (April 2021)
UKCCIS Guidance on Sexting in Schools and College (2016)
Teaching Online Safety in Schools (June 2019)
Safeguarding and remote education during Coronavirus (Covid 19), DfE, (April 2020)
The use of social media for online radicalisation (July 2015)
DfE: Relationships Education, Relationships and Sex Education (RSE) and Health Education (Sept 2020)

See also the School's policies as follows:
Safeguarding and Child Protection Policy, Staff Procedures Handbook, Staff Code of Conduct, Anti-Bullying Policy, Anti-Cyber Bullying Policy, Whistleblowing Policy and Procedures and Implementing Prevent Policy, Record Retention Policy

Definitions or abbreviations used in this policy
CEOP: Child Exploitation and Online Protection Centre
DFE: Department for Education
DPA: Data Protection Act
DSL: Designated Safeguarding Lead
EYFS: Early Years Foundation Stage
IT: Information Technology
ISP: Internet Service Providers
KCSIE: Keeping Children Safe in Education
LBRUT: London Borough of Richmond upon Thames
PSHEE: Personal, Social, Health and Economic Education
UKCCIS: UK Council for Child Internet Safety
URL: Uniform Resource Locator
WSUS: Windows Server Update Service

At Kew College Prep
DSL: Robyn Hodgson
Deputy DSL and Head: Jane Bond
Deputy DSL Early Years: Stephanie Aird

1. INTRODUCTION

Use of the Internet is continually expanding and has become an important part of learning and communication. The Internet has no boundaries and we are aware that our pupils may be influenced by what they see and who they communicate with. It brings our pupils into contact with a wider range of information which may or may not be appropriate for the age of our pupils.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using IT. When distributing the curriculum, teachers need to prepare for and make use of communications technology i.e. web-based resources, email and live instant messaging communication. Access to life-long learning and enhancement of employment requires computer and communications use and pupils at Kew College Prep need to learn about and develop these skills. Through the use of Internet based activities those adults supporting learning within Kew College Prep are able to enrich the range of opportunities and resources available to pupils. They should be equally aware of the risks as well as the opportunities presented. It is essential that both staff and pupils are protected from the dangers of the misuse of technology and that pupils are taught how to use technology safely and are made aware of different risks that are posed online, in an age appropriate manner.

The School's Internet and Online-Safety Policy relates to other policies including those for safeguarding of children, behaviour and PSHEE.

2. THE INTERNET IN THE SCHOOL

2.1. Rationale and Entitlement

The purpose of Internet access in Kew College Prep is to raise and develop the achievement and skills of pupils, to support the professional work of staff and to enhance the School's management information and business administration systems. Access to the Internet is a necessary tool for all staff and pupils irrespective of gender, race, religion, culture or ability. It is an entitlement for pupils who show a responsible and mature approach with the intention to gain useful or engaging resources. Appropriate use of the Internet provides a number of benefits to our pupils and staff. These benefits include:

2.2. Resources

- Providing access to documentation including on-line publishing of documents (schools' policies, lesson plans, activities, etc)
- Providing support and documentation for software updates
- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives and the Learning Platform
- Information and cultural exchanges between pupils worldwide
- Discussion with experts in many fields for pupils and staff

2.3. Staff Professional Development

- Access to educational materials
- Sharing good practice with colleagues

- Communication with the advisory and support services, professional association and colleagues

2.4. Administration

- More regular communication with schools and more immediate responses to inquiries
- Access to technical support including remote management of networks
- Method to publish information to schools that will free more resources for teaching and learning
- Management of the School network from a single source, thus reducing the overall cost of performing this role
- Added value through the creation of a secure effective communication system between Kew College Prep and the LBRUT, between Kew College Prep the Independent Schools Inspectorate and between Kew College Prep and other schools that can improve the transfer of information and data

2.5. Email

- Provision of a quick method of communication
- Provision of a centrally maintained email system that can give pupils an email address that will remain constant throughout their education at Kew College Prep

2.6. Security provisions at the School as part of the Safeguarding Framework

- Provision of a buffer between Kew College Prep and the Internet which is designed to ensure children are safe and enhance performance
- Real time monitoring with automated alerts through Netsupport DNA
- Secure appropriate filtered internet access and content, i.e. preventing pupils from viewing extremist content leading to radicalisation
- Back up filtering and blocking using a second application without over blocking
- Monitored email for pupils
- Email anti-virus – to scan all unencrypted external and internal email delivered to the Kew College Prep Network, using anti-virus system that are kept constantly up to date
- Microsoft Critical Updates: distribution of Microsoft critical security updates services WSUS (School's responsibility to ensure computers are kept updated)
- Statutory UK ISP monitoring laws – Records all Internet usage and email. The Head of the School will be informed when grooming or abuse is suspected

2.7. Aims

At Kew College Prep our aims are:

- To use the Internet safely and effectively
- To limit the children's exposure to illegal, inappropriate or harmful material
- To prevent pupils from being subjected to harmful online interaction with other users
- To ensure every pupil can use the internet safely and responsibly
- To protect the School, its staff and pupils from undesirable content
- To raise the awareness of staff and students to the benefits of Internet access
- To develop a School website to serve the School community and prospective parents

2.8. Objectives

At Kew College Prep our objectives are:

- To promote the use of the Internet as a learning tool
- To educate the users in safe use of the internet
- To assess the risks posed by those at School and adjust the technology and policies accordingly
- To promote a learning platform environment
- To develop the skills in our pupils necessary for the creation of websites

3. RESPONSIBILITY

Clearly defined roles and responsibilities for online safety as part of the School's wider safeguarding strategy and how this links with our safeguarding policy;

The Head and Designated Safeguarding Lead (DSL), have the prime responsibility for ensuring that:

- Staff and pupils are protected from the misuse of technology including the use of mobile telephones and cameras
- Pupils are educated in an age appropriate manner to keep themselves safe and understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults and to adjust their behaviour as necessary
- The systems and procedures in School have the highest security settings and filters are in place to ensure that children are safe from inappropriate sexual, terrorist and extremist material when accessing the internet in School and these filters are regularly checked
- Internet safety is included in staff professional development and safeguarding training and that parents are included in awareness of online safety.

The Director of Studies has the delegated responsibility to ensure that the curriculum throughout the School makes the best use of technology and the pupils follow appropriate programmes of study both to develop the necessary technological skills and to keep themselves safe.

The Deputy Head, Head of Infant House and Head of EYFS have the responsibility for ensuring that the School's policies are being followed.

All staff have a responsibility to the School community as a whole. As well as ensuring that their own practice follows School policy, should they have any concerns about a colleague or pupils putting themselves or the School at risk then this must be discussed with the relevant Deputy Head (see ***Whistleblowing Policy***.)

4. USE OF TECHNOLOGY IN THE CLASSROOM

There is clear guidance on the use of technology in the classroom and beyond for all users, including staff, pupils and visitors that references permissions/restrictions and agreed sanctions.

Access to the Internet is supervised at all times.

Pupils in Years 3 to 6 are instructed in acceptable (i.e. responsible and safe) use of the Internet. Pupils from Year 3 upwards have their own School based individual email account. The IT Manager speaks to all pupils in Year 3 and above at the beginning of each academic year about appropriate use and ensures throughout the year that safe use of the internet is taught and understood by the pupils. Parents are sent the "Rules for Pupils" and required to sign the "Responsible Internet Use" forms before their children are allowed to use the internet. Pupils are informed that their Internet use will be monitored at all times.
Each time a pupil logs in to their own account, they are shown a reminder of the school rules and regulations which they must agree to before logging into the system.

4.1. Assessment of risks

The School takes reasonable precautions to ensure that users access only appropriate material. No pupils are allowed to load software or use discs or memory sticks in School. Virus protection has been installed on all School computers and laptops and is updated regularly.

5. USE OF TECHNOLOGY BY STAFF IN AND BEYOND THE CLASSROOM

School administration staff, teaching staff and pupils may have access to the School's internet system outside the classroom. However, no visitor or parents should be given the log in codes. Children should never share their log in codes for Teams, our platform for online, remote learning.

At the beginning of each academic year, all staff are provided with this Policy and its importance is explained. Staff's attention is drawn to the relevant changes to the policy each year. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Professional conduct is essential.
Each time a member of staff logs on to their own account, they are shown a reminder of the school rules and regulations which they must agree to before logging into the system.

5.1. Staff management of email

Staff have their own School email addresses. Staff are discouraged from using the School email system for personal use and are made aware that all usage may be monitored. Unknown attachments should not be opened. Inappropriate use of the School email system may result in email access being withdrawn and disciplinary action being taken. Any use of any email at School should be appropriate. The forwarding of chain letters is not permitted. Any e-mail message which is abusive, discriminatory on grounds of sex, marital status, race,

disability, sexual orientation or religious belief, or defamatory is not permitted. Use of the e-mail system in this way constitutes gross misconduct.

Email sent to an external organisation or individual (for example a parent) should be written carefully before sending, in the same way as a letter written on School headed paper. Where necessary, emails to parents and external parties are first reviewed by the Deputy Head or Head. Staff should never respond to an email in haste or anger and if need be should wait 24 hours before responding. Should an email be received that could be considered a complaint, staff should always inform the Head immediately. Staff should bear in mind that whatever they write in an email may – through no fault of their own – end up being seen by someone who is not the intended recipient, and may be required as a disclosure in an open court in any litigation.

Staff should also be aware, all individuals whose data is held by the School, have a legal right to request access to such data or information. This is a Subject Access Request (SAR). The School shall respond to such requests within one month. This will include data held in emails.

All external e-mail correspondence should contain the School's disclaimer:
This email is for the use of the intended recipient(s) only. If you have received this email in error, please notify the sender immediately and then delete it. If you are not the intended recipient, you must not keep, use, disclose, copy or distribute this email without the author's prior permission. Kew College Prep has taken precautions to minimise the risk of transmitting software viruses, but we advise you to carry out your own virus checks on any attachment to this message. We cannot accept liability for any loss or damage caused by software viruses.

5.2. Staff use of School computers

5.2.1. ***Property:*** Any property belonging to the School should be treated with respect and reasonable care and any faults or breakages should be reported immediately through the IT Helpdesk system. Staff should not use the School's computers unless they are competent to do so and should ask for training if required.

5.2.2. ***Viruses***: Staff should be aware of the potential damage that can be caused by computer viruses. They must not introduce or operate any programmes or data (including computer games) or open suspicious e-mails which have not first been checked by the School for viruses. Staff have been trained on how to move unwanted mail to their 'junk' folder and the IT Manager can centrally block recurring spam emails that are of nuisance.

5.2.3. ***Passwords***: Passwords protect the School's network and computer system. They should not be obvious, for example a family name or birthdays. Staff should not let anyone else know their password and must immediately inform the IT Manager and the Head if it appears to be compromised. Staff should not attempt to gain unauthorised access to anyone else's computer or to confidential information which they are not authorised to access.

5.2.4. ***Leaving workstations***: If a workstation is left for any period of time the user should log off. The computers automatically turn off every night.

5.2.5. ***Use of Mobile Technology by staff***
Staff can only access the School network offsite through a secure log on. Any photographs taken for School purposes must only be stored on the School network and not on any personal device.

5.3 Online Safety and Remote Learning

5.3.1 As set out in KCSIE (2021) guidance, Kew College Prep online safety is the responsibility of the Designated Safeguarding Lead who works with staff to promote safe practice across the school and with parents and pupils to support safe practice at home.

5.3.2 In line with the DFE's Guidance Teaching online safety in school (June 2019), pupils are taught about online safety and harms in their IT lessons, through their PSHEE lessons and through Relationships Education in an age appropriate way. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. They are taught the underpinning knowledge to help them navigate the online world safely and confidently regardless of the device, platform or app. This includes:

- how to help them evaluate what they see online
- how to recognise techniques used for persuasion
- how to identify online risks
- to understand what acceptable and unacceptable behaviour looks like, and
- how and when to seek support.

5.3.3 At induction and through regular annual training, staff are trained in the role of technology in both safeguarding and wellbeing issues, and that online abuse can occur in tandem with face to face abuse. Any concerns related to online abuse will be dealt with in line with Kew College Prep's Safeguarding and Child Protection Policy. Referrals will be made to Richmond and Kingston SPA, and the police may also be contacted when deemed necessary and appropriate.

Children who are working online in school or at home, have clear reporting routes to staff so that they know who they can turn to in the event of online abuse or feeling unsafe online. Parents, pupils and staff are aware of the role of the DSL and Deputy DSL in reporting online safety matters.

5.3.4 Child Sexual Exploitation and Child Criminal Exploitation can be facilitated through online platforms such as the Web and Social Media Apps. Peer on peer abuse and initiation or hazing type of violence and rituals may include an online element. It is important that parents are aware of their child's online activity which extends beyond the school's online learning platform. Parents, carers, teachers and other Kew College Prep staff should immediately draw to the attention of the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead any activity that might be related to CSE and/or CCE. Parents have the option to reach out to a range of support organisations including the Richmond

and Kingston SPA. Kew College Prep, via the National Online Safety platform, provides a wide range of informational video clips and courses to support our parent community to recognise, respond to and manage suspected Child Sexual or Child Criminal Exploitation.

5.4 Procedures adopted to safeguard children while learning remotely.

At times, it may be necessary for Kew College Prep pupils to receive their lessons via a secure remote learning platform. Every year, Kew College Prep provides guidance for its parents for keeping our children safe online whilst working at home, together with colourful posters for pupils highlighting key points for keeping them safe online. Parental consent is required for children to participate in online schooling and to submit videos and pictures of themselves; this consent can be changed at any time through Schoolbase.

Information is also provided to parents on the form of lessons to be provided (for example, live stream lessons or pre-recorded lessons) and the conduct expected of staff, pupils and parents. Staff are trained with regard to the appropriate use of using pre-recorded videos/Powerpoint presentations, live lessons and/or photographs to support learning. Remote teaching will include both recorded or live direct teaching time, and time for pupils and students to complete tasks and assignments independently. Microsoft Teams is the learning platform used by the Kew College Prep community for remote learning. It is centrally secured, and safe for children and staff to use.

To safeguard children and staff, live lessons adhere to the following rules which are communicated to staff, parents and pupils:

- use neutral or plain backgrounds
- ensure appropriate privacy settings are in place
- ensure staff understand and know how to set up and apply controls relating to pupil and student interactions, including microphones and cameras
- set up lessons with password protection and ensure passwords are kept securely and not shared *
- ensure all staff, pupils, students, parents and carers have a clear understanding of expectations around behaviour and participation

5.5 Communicating with parents, carers, pupils and students

Where education is taking place remotely due to coronavirus (COVID-19), Kew College Prep maintains professional practice at all times. When communicating online with parents, carers, pupils and students, the following should be adhered to at all times:

- communicate within school or college hours as much as possible (or hours agreed with the school or college to suit the needs of staff)
- communicate through the school or college channels approved by the senior leadership team
- use school or college email accounts (not personal ones)
- use school or college devices over personal devices wherever possible
- advise staff not to share personal information

- ensure parents and carers are clear when and how they can communicate with teachers (resources to support communications are available)
- ensure logins and passwords are secure and pupils and students understand that they should not share this information with others

Teachers should try to find a quiet or private room or area to talk to pupils, students, parents or carers. When broadcasting a lesson or making a recording, consider what will be in the background.

5.6 Use of Pupil Images for Remote Learning

- ***Pre-recorded videos/PowerPoint presentations and photographs of pupils to support remote learning*** - Pre-recorded videos/PowerPoint presentations and photographs of pupils will be kept for the academic year and then securely deleted
- ***Recording of Remote Lessons to allow pupils to re-work through the lessons in their own time*** – if the lesson is recorded, it will only contain pupil's voices but not images of pupils. Lessons that are recorded are kept for the academic year and then securely deleted
- ***Livestreaming of PSHEE lessons from the classroom to allow a pupil to join the lesson from home*** - the lesson will contain pupil's voices and images. These lessons are not recorded

5.7 Remote meetings with parents

- ***Remote meetings with parent groups***: If meetings are to be recorded for dissemination to other parents, this will be advised to all parents when the meeting is set up.
- ***Remote on-line one-on-one parent meetings:*** Unless for a specific purpose and agreed by both parties or for safeguarding reasons, parent one -on-one meetings, including Parent's Evenings meetings are not recorded. Parents will be told in advance that the school will not be recording the meeting and that parents do not have the school's permission to record the meeting.

6. TECHNICAL PROVISION

Filtering is provided by Lightspeed, firewalled by Schoolcare to ensure staff and pupils are protected, content reviewed and sites blocked. The filtering software, used and monitored by the Kew College Prep Network, contains a number of lists or categories of URLs that can be marked as allowed or denied. These lists are updated frequently. Any unsuitable sites that are discovered by pupils or staff are reported to the IT Department; it is then reported to the ISP to add to the block list.

Sites that are within disallowed categories are blocked automatically. This mechanism provides an additional 'safety' check. It also allows for many more sites than would conventionally be available, using the simple 'allowed list' system used by other filtering applications.

None of these systems can be completely effective in isolation therefore a combination of approaches is used. It is acknowledged that adequate supervision is essential.

No pupil or member of staff may access inappropriate sites of any sort, and staff misuse of the internet may result in disciplinary proceedings, including those for gross misconduct.

7. EDUCATING PUPILS

7.1. The importance of Internet use and its benefit to education

Internet use is a part of the curriculum and a necessary tool for pupils. It is an essential element of education and the School has a duty to provide pupils with Internet access as part of their learning experience. The internet provides access to world-wide educational resources, for example museums, art galleries as well as subject-specific websites.

7.2. Using the Internet to enhance learning

School Internet access has been designed for pupil use and includes filtering appropriate to the age of the pupils. Pupils are taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Staff guide pupils in on-line activities and educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

7.3. Pupils evaluating Internet content

In the unlikely event of staff or pupils discovering unsuitable sites, the URL (address) and content must be reported to the IT Manager who will ensure that it is reported to the Internet Service Provider. The School ensures that the use of Internet-derived materials by staff and pupils complies with copyright law. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils are taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

As part of the PSHEE provision at Kew College Prep, the Relationships Education curriculum and the IT curriculum children are taught how to keep themselves safe on line and to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults. In the first ICT lesson of the academic year 'Internet use – Rules for Pupils' and the wording in the Acceptable Use Policy (which pupils and staff agree to every time they log onto a School computer) are discussed with all pupils. Any pupil that misses this lesson has a one-on-one meeting with the ICT teacher to discuss these matters.

Children from Year 3 sign an internet agreement where they agree not to use the internet inappropriately. In addition, presentations are periodically made in assembly using age appropriate material.

The dangers of radicalisation by online media are taught in Computing lessons, with the ideology behind the Prevent strategy being taught across the curriculum to Year 6.

Latest resources promoted by DFE can be found at

The use of social media for on-line radicalisation (https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation)DfE: Teaching online safety in school (June 2019)

The UK Safer internet Centre (www.saferinternet.org.uk)

CEOP's thinkyouknow website (www.thinkyouknow.co.uk)

In addition, the following resources are used;

www.kidsmart.org.uk

www.childnet.com

7.4. Use of Mobile Technology by pupils

The use of personal devices, such as mobile phones, iPads, tablets or laptops, by pupils is not allowed in School. Pupils in Year 6 only, who wish to bring a mobile phone to School in the Summer Term must hand it in to the School office upon arrival at School and may then collect it at the end of the day. No other pupil is permitted to bring a mobile phone to School. Certain pupils are allowed to use a laptop in lessons and/or exams because of specific learning difficulties; however, pupils are not allowed to use the School network on their own devices. Children should be aware of the dangers of sexting. See Safeguarding and Child Protection Policy.

No child should have a mobile phone on their person or in their bag during School hours. If a pupil is found to have one, it is removed, held in the office and handed to the parent, guardian or carer the end of the day. The child will be disciplined in accordance with the School Good Behaviour and Discipline Policy.

The School owns a number of iPads for pupils' use in supervised situations only.

8. STAFF PROFESSIONAL DEVELOPMENT

New staff are introduced to the School's systems as part of their induction training. Should they require further training they should contact the IT Manager.
In addition, safe internet use is a regular feature of staff safeguarding training which is compulsory every year.

The Deputy Head/IT manager also arranges for staff IT training periodically either as part of or in addition to regular staff meetings.

The Prevent Strategy, incorporating online radicalisation, is known to all staff following workshops and online tutorials.

9. REPORTING MECHANISMS

There are various reporting mechanisms in School that should be used as follows:

- Termly risk assessments - these should refer to any technology in the relevant area including electrical hazards, trip hazards
- An IT Helpdesk for speedy electronic reporting of maintenance issues
- Pupil Misuse: Any complaints about pupil misuse should be referred to the IT Manager and to the Designated Safeguarding Lead in the first instance, and to the Head if relevant. Sanctions available include the removal of Internet or computer access for a period, or more serious sanctions could result in suspension or exclusion.
- NetSupportDNA provides updates on a daily basis of items reported to the IT Systems Manager and for more serious issues to the Deputy Head and the Head for clearance. Any safeguarding issues will immediately be reported to the DSL, who will deal with the matter in accordance with the Schools Safeguarding and Child Protection Policy.
- Concerns over the use of IT, including use of mobile telephones and cameras, sending of images via the internet or by texting, inappropriate material appearing on the screen, inappropriate use of IT by a pupil, parent or staff member, must be reported immediately to the Deputy Head unless this comes under child protection in which case the Head and DSL should be informed immediately. If the concern is about the Head, then the Chair of Governors should be contacted without the Head being informed.
- Children who are working online have clear reporting routes to staff so that they know who they can turn to in the event of online abuse or feeling unsafe online.

10. INFORMING PARENTS

The School provides an evening talk for parents on online Safety which is delivered by outside providers.

Parents must be informed of any misuse by their child of the School's internet and networking system. This should be done through the Head of Pastoral Care.

11. MANAGEMENT OF PERSONAL DATA

The School has a need to process personal data and follows the principals of the Data Protection Act (DPA) and General Data Protection Requirements to ensure that personal data:

- Is processed fairly and lawfully
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes
- Is accurate and, where necessary, kept up to date

- Is adequate, relevant and not excessive in relation to the purposes for which it is processed
- Is not kept for longer than is necessary for those purposes
- Is processed in accordance with the rights of data subjects under the DPA
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

For the purposes of the Data Protection Act 1998 ("the DPA"), Kew College Prep ("the School") is the "data controller" of personal data about pupils and their parents and/or guardians.

11.1. Personal data processed by the School

Personal data processed by the School includes contact details, national curriculum and other assessment results, attendance information, special educational needs, and images of pupils engaging in School activities and, in relation to parents and/or guardians, may include financial information. The School may also process sensitive personal data such as ethnic group, religious beliefs and relevant medical information. Personal data will usually be collected directly from parents / guardians, but some may be passed to the School by third parties.

11.2. Purposes for which personal data may be processed

Personal data (including sensitive personal data, where appropriate) is processed by the School strictly in accordance with the Data Protection Act in order to:

- Support its pupils' teaching and learning
- Monitor and report on their progress
- Publish examination results [as separately notified to affected pupils and/or their parents and/or guardians]
- Provide appropriate pastoral care
- Assess how well the School as a whole is doing
- Communicate with former pupils
- Monitor pupils' email communications, internet use and telephone calls for the purpose of ensuring compliance with the School's Online Safety and Cyber Bullying Policies
- Where appropriate, promote the School to prospective pupils (including through the School's prospectus, School Magazine and website), and
- Other reasonable purposes relating to the operation of the School.

Pupils and their parents and/or guardians, as data subjects, have certain rights under the DPA. The presumption is that by the age of 12 a child has sufficient maturity to understand his/her rights and to make an access request themselves if he/she wishes. A parent would normally be expected to make a request on a child's behalf if the child is younger.

12. WEBSITE

The Head with the assistance of the Senior Leadership Team has overall responsibility for overseeing the website, and ensuring consistently high standards. All members of staff who upload content should take care that all material is appropriate and carefully edited. Any pupil's work that is used for internal purposes and for the School community should contain only the Year group and the pupil's first name and Surname initial, e.g. "John W, Year 5". Images should be selected for appropriate use and represent the whole School, not just individuals who are photographic. Images on the public part of the website can only be used of pupils where photographic parental consent has been received.

Reviewed by:	**Reviewed and Approved by:**	**Updated by:**
The Education and Welfare Committee	Name: Jane Bond	Name: Laura Liguori
	Title: Head	Title: Designated Safeguarding Lead
Date: 17 Nov 2021	Date: 1 Sep 2022	Date: 15 May 2022

This policy will be reviewed by the governing body every 3 years or earlier if it is considered necessary.

KEW COLLEGE PREP

Internet use – Rules for Pupils

These rules will help us to be fair to others and keep everyone safe.

The following rules apply to all children in Years 1 - 6:

- I will only use the School computer network and Internet for learning
- I know that the School may check my computer files and the Internet sites that I visit
- I will only use the internet when an adult is with me and I have permission
- I will always ask if I get lost on the Internet
- I will only click on the buttons or links when I know what they do
- I will tell an adult if I see anything I am uncomfortable with or that breaks these rules

The following additional rules apply to children in Years 3 - 6:

- I will only send and open emails when an adult is with me
- I will only write emails to people that I know
- I will send e-mails and attachments that are polite and friendly
- I will not open e-mails sent by anyone I don't know
- I will not use any web-based email
- I will only use apps that are authorised by a member of staff
- I will immediately close any webpage I am not sure about
- I will not bring software into School
- I will not bring disks or Memory Sticks into School except with prior permission
- I will not use any personal device to connect to the School internet or network
- I will not use any social media sites
- I will not use Internet chat rooms
- I will never share personal information or passwords with other people
- I will never arrange to meet anyone I don't know
- I will not look at, or change other people's files without their permission
- I understand that I should hand in to the School Office any personal mobile device which has the capacity to access the internet or take photographs, and that I must not use any such device at School, on School trips or at games, etc.
- I understand that if I break these rules, I could expect to be disciplined according to the School's current policies and that my parents will be informed.

The School may exercise its right to monitor the use of the School's computer systems, including access to web-sites, the interception of E-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text or imagery

KEW COLLEGE PREP

Responsible Internet Use Agreement

Dear Parent,

As part of your child's curriculum and the development of IT skills, the School provides supervised access to the Internet. We believe that the use of the World Wide Web and email are worthwhile and are essential skills for children as they grow up in the modern world.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to deal with this risk at School. Our School Internet provider operates a filtering system that restricts access to inappropriate materials. We have dedicated monitoring software, that automatically blocks and flags up potential unsuitable content. This may not be the case at home, and we can provide references to information on Safe Internet Access if you wish.

At School, Net Support DNA safeguarding system is live and monitored by Systems manager. Net Support DNA monitors keywords and phrases to alert schools of any online activity, either by staff or pupils that may have Online-Safety or safeguarding issues. The Systems Manager and Designated Safeguarding Lead review the findings on a regular basis and report to the Head.

Pupils in Years 1-Year 6 have been given a presentation to help them understand the Kew College Prep Online-Safety Rules and Agreement at age appropriate levels.

Both pupils and their parents/carers are asked to read the enclosed Rules for pupils for Responsible Internet Use, and sign to show that the Online-Safety Rules have been understood and agreed. Parent and pupil consent is required so that your child may use the Internet at School. Pupils are asked to acknowledge these rules every time they access the School network.

Should you wish to discuss any aspect of Internet use, please contact the Head on the following email: Path@kewcollege.com

Yours sincerely,

IT Manager

Pupil's Responsible Internet Use Agreement	
Pupil:	Class:
• I have read and I understand the School Rules for Responsible Internet Use. • I will use the computer, network, mobile phones, Internet access and other technologies in a responsible way and obey these rules at all times. • I know that the School may check my computer files and the Internet sites that I visit	
Signed	Date:

Parent's Consent for Internet Access

I have read and understood the School Rules for Responsible Internet Use and give permission for my son / daughter to access the Internet. I understand that whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, I appreciate that this is a difficult task. I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the School will not be liable for any damages arising from my child's use of the Internet facilities.

Signed: …….. Date:

Please print name: ……

Please complete, sign and return to the class teachers by XXXXXXX