Kenton College Preparatory School

E-safety & Acceptable Internet & iPad Use Policy

Audience	Teachers, Parents, Governors
Author	Deputy Head Pastoral
Last Review	October 2025
Next Review	October 2026
Related Policies	Child Protection & Safeguarding Policy Staff Code of Conduct

Introduction

The Board of Governors and staff of Kenton College take seriously their responsibility for safeguarding and promoting welfare of all pupils in their care. The Kenton College Board of Governors are ultimately responsible for the provision stated in this policy.

Kenton is committed to:

1. preparing pupils to be confident and productive users of online platforms and technology.
2. teaching pupils to be safe online, including giving them an appreciation of how to maintain a healthy digital footprint.

To that end, this policy sets out the guidelines and protocols for achieving the above.

Glossary of Terms

For clarity, this policy uses the following terms unless otherwise stated:

Users - refers to staff, Governors, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits and trips

Wider school community – pupils, all staff, Governors, parents

Safeguarding is a serious matter at Kenton. We use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

This policy is available for anybody to read on the school website. Upon review, all members of staff will sign to acknowledge that they have read and understood this policy.

Roles & Responsibilities

Board of Governors

The Board of Governors is accountable for ensuring that Kenton has effective policies and procedures in place. The Senior Leadership Team (SLT) will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- The Designated Safeguarding Governor will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher regarding training, identified risks and any incidents.
    - Meet regularly with the Designated Safeguarding Lead.
    - Ensure online safety incidents are featured in the annual safeguarding report.
    - Report to relevant Governors / Board / Committee / meeting.

Headteacher & Senior Leadership Team

Reporting to the Board of Governors, the Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to the Deputy Head Pastoral, who liaises with the Head of ICT, ICT Manager and Heads of Year.

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and Board of Governors and parents.
- An online safety expert will visit Kenton and deliver talks to pupils, parents and staff.
- All online safety incidents are dealt with promptly and appropriately.
- The Headteacher and all relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Deputy Head Pastoral

- Keep up to date with the latest risks to pupils whilst using technology (familiarising themselves with the latest research and available resources for school and home use).
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher (and Board of Governors) on all Online Safety matters.
- Engage with parents and the school community about Online Safety matters at school.
- Liaise with the ICT Manager as required.
- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Provides training and advice for staff (or an external provider would provide this)
- Will be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data and images
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming including radicalisation
- online-bullying

ICT Manager

Technical support staff are responsible for ensuring that:

- The ICT technical infrastructure is secure; this will include at a minimum:
  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - The school internet operating system is updated regularly.
  - Any Online Safety technical solutions such as Internet filtering are operating correctly.
  - Filtering levels are applied appropriately and according to the age of the user by liaising with the Deputy Head Pastoral and the Headteacher.
  - Passwords are applied correctly to all users regardless of age.
  - Ensure any technical Online Safety measures in school are fit for purpose.
  - Networks and devices through a properly enforced password protection policy.
  - Regular checks are carried out on iPad use.

All Staff

Staff are to ensure that:

- They have an up to date awareness of online safety matters and of the current Online Safety Policy and practices.
- All details within this policy are understood. If anything is not understood it should be brought to the attention of the relevant member of staff.
- Any online safety incident is reported to the Deputy Head Pastoral.
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Pupils will understand the appropriate use of AI.
- Monitor the use of digital technologies in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- The boundaries of use of ICT equipment and services in this school are given in the pupil Acceptable Use Policy. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- Online Safety is embedded into our curriculum. Pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.
- Pupils will be expected to know and understand policies on the taking / sharing / use of images and on online bullying.

- Pupils should understand the importance of adopting 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, if related to their membership of the school.

Parents and Carers

Parents play the most important role in the development of their children. As such the school will support parents to ensure the safety of children outside the school environment. Through parent in partnership sessions, school newsletters, letters and parent portal, the school will keep parents up to date with new and emerging Online Safety risks. The school will encourage parents to adopt strategies to enable them to monitor and control their child's online activities.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Internet Filtering
We use Sophos XGS 2300 Unified Threat Management(UTM) Firewall software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites (appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner.) The Deputy Head Pastoral and ICT Manager are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering
We use the Gmail Google Workspace for Education application with built in antivirus scanning which prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption
All school devices that hold personal data (as defined by the Data Protection Act 2019) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or school mobile phone) is to be brought to the attention of the Headteacher immediately.

Passwords
All staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change if there has been a compromise. The ICT Manager and Support Team will be responsible for ensuring that passwords are changed.

Anti-Virus
All capable school managed devices have Symantec Endpoint 14 anti-virus software. The virus definition deployments are centrally managed with daily updates. Additionally the Sophos XGS 2300 UTM will scan all content transmitted to and from the internet for malware with similar daily updates. The ICT Manager will be responsible for ensuring the antivirus software is updated and upgraded as necessary and will report to the Headteacher if there are any concerns.

Regular Monitoring
School ICT technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

Safe Use

Internet
Use of the Internet in school is a privilege, not a right. Internet use will be granted to:

- Staff upon signing an Online Safety and the staff Acceptable Use declaration.
- Pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Email
All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted and work email addresses should not be used for any personal purpose. Whilst pupils have an email capable account (following the system: firstname.surnameyear of graduation@students.ac.ke), it is only used as part of their access to the school network - the email function is disabled and therefore not able to send or receive emails.

Photos and videos
Digital media such as photos and videos are covered in the schools' Data Protection Policy and are reiterated here for clarity. All parents must sign a photo and video Consent Form at the time of their child's admission to Kenton and annually thereafter. Photos and videos are used for school publications, the website and other educational purposes such as assemblies. All safeguarding and data protection laws and protocols are observed.

Incidents
Any online safety incident is to be brought to the immediate attention of the Deputy Head Pastoral or the Headteacher.

Training and Curriculum
It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology. This includes updated awareness of new and emerging issues. As such, Kenton will have an annual programme of training which is suitable to the audience.

Online Safety for pupils is embedded into the curriculum and is taught specifically in ICT lessons. Whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Pupils cover Online Safety sessions in the school's Wellbeing Programme and it is also embedded in the Computing Curriculum.

The Deputy Head Pastoral is responsible for recommending a programme of training and awareness for the school year to the Headteacher. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area, this must be brought to the attention of the Headteacher for further CPD.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should complete online safety training (via EduCare) as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Deputy Head Pastoral will sensitise staff to changes on online safety as part of the KCSIE updates.
- This Online Safety Policy and its updates will be presented to and discussed by staff in CPD meetings / INSET days.
- The Deputy Head Pastoral will provide advice / guidance / organise training to individuals as required.

iPads

iPads may be school owned/provided or personally owned. Kenton pupils use iPads that have the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform (Google Classroom) and other cloud-based services such as Google Drive.

Pupils in Years 2 - 4 use a class iPad owned by Kenton. These class sets of iPads remain in school and are assigned to each pupil at the start of the academic year.

Pupils in Years 5 - 8 use a personal iPad / device that is purchased by parents. A list of required apps for use in school are provided to parents. The iPads / devices are protected by the school's internet filtering systems when they are connected to Kenton's wireless network.

In all cases, the iPad (whether school-owned or personal) must be secured in a protective casing and have a screen protector. Failure to adhere to this may compromise any insurance claims if damage occurs to the iPad.

Occasionally, in liaison with the Learning Support Department and/or Head of Year, a pupil may be permitted to use a laptop instead of an iPad.

All users should understand that the primary purpose of the iPads and laptops in a school context is educational. Teaching the safe and appropriate use of mobile technologies is an integral part of the

school's Online Safety education programme. This is integrated as a strand in Computing (Digital Literacy and Citizenship).

Once a term, Kenton will observe a 'Tech-Free Week' which parents will be encouraged to support at home. Pupils will not be set homework (Prep) on iPads.

Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the Headteacher or Deputy Head Pastoral any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature.
- Any digital communication between staff to pupils or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Teachers communicating to a whole class must do so through Google Classroom.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details in communications. They are taught to report inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the school website and only official email addresses should be used to identify members of staff.

- An external provider is invited into Kenton to talk to parents and pupils about Online Safety.

Staff with Personal Social Media accounts

- In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school network will not allow access to social media sites via the wireless network.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing illegal images or distributing racist material is illegal and is banned from school. Other activities e.g. online bullying are banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The following activities referred to in the section below are unacceptable and inappropriate in a school context. No member of staff should engage in these activities in or outside the school. The school policy restricts usage as follows:

Activity	Notes
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act (UK, 1978)	Unacceptable & illegal
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act (UK 2003)	Unacceptable & illegal
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act (UK, 2008)	Unacceptable & illegal
Criminally racist material in UK – to incite religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act (UK, 1986)	Unacceptable & illegal
Pornography	Unacceptable
Promotion of any kind of discrimination	Unacceptable
Threatening behaviour, including promotion of physical violence or mental harm	Unacceptable
Promotion of extremism or terrorism	Unacceptable
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	Unacceptable
Using school systems for a private business	Unacceptable
Infringing copyright	Unacceptable
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)	Unacceptable
Creating or propagating computer viruses or other harmful files	Unacceptable

School Actions & Sanctions

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the school's normal behaviour / disciplinary procedures and dealt with as a school issue unless referral and reporting to outside agencies and the police is deemed necessary.

A pupil is likely to be banned from using their iPad for a fixed period of time (other sanctions may apply) and parents will be informed if their child does any of the following:

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised inappropriate use of mobile phone or other mobile device
- Unauthorised/ inappropriate use of social media, messaging apps, personal email
- Allowing others to access the school network by sharing username and password
- Attempting to access or accessing the school network, using another pupil's account
- Accessing another pupil's account without permission
- Corrupting or destroying the data of other users
- Sending any digital message that is regarded as offensive, harassment or of a bullying nature
- Deliberately accessing or trying to access offensive or pornographic material

A member of staff may invoke the disciplinary procedure if they do any of the following:

- Deliberately accessing or trying to access material that could be considered illegal
- Intentional deletion of school files
- Inappropriate personal use of the internet, social media or personal email
- Unauthorised downloading or uploading of confidential files/information
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email, social networking, instant messaging or text messaging to carry out digital communications with pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material

Acceptable Internet Use for Staff

Note: All Internet and email activity is subject to monitoring

Internet access: Staff must not access or attempt to access any sites that contain any of the following: child abuse, pornography, promoting discrimination of any kind, promoting racial or religious hatred, promoting illegal acts or any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident and reported to the Headteacher/Deputy Head Pastoral.

Social Media: Staff using Social Media for personal use should never undermine the school, its staff, parents or pupils. Staff should not become "friends" with pupils on personal social networks.

Use of Email: Staff are not permitted to use their school email addresses for personal business unless with approval from the Headteacher. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords: Staff should keep passwords private. There is no occasion when a password should be shared with another member of staff or pupil. On occasion it may need to be shared with IT support.

Data Protection: If it is necessary for staff to take work home or off-site, they should ensure that their device is encrypted. On no occasion should data concerning personal information be taken off-site on an unencrypted device.

Personal Use of School ICT: Staff are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos: Staff should not upload onto any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT: Use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment.

Viruses and other Malware: Any virus outbreaks are to be reported to the ICT Manager who will then take appropriate measures to mitigate the exposure of the school and greater community, report it to threat management providers as soon as it is practical to do so, along with any samples (if practical) and state actions undertaken by the school.

Online Safety: Like Health and Safety, Online Safety is the responsibility of everyone. As such, staff will promote positive Online Safety messages in all use of ICT whether they are with other members of staff or with pupils.

Acceptable Use Policy – pupils

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I promise – to only use the school ICT for school work that the teacher has asked me to do.

I promise – not to look for or show other people things that may be upsetting.

I promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment. If I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download or stream anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Kenton ensures that:

- It has a Data Protection Policy.
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data to minimise the risk of its loss or misuse.
- Only use personal data on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

Bring Your Own Device (BYOD) Rules for Senior Pupils

The iPad/Device is for school use. It is not a toy and should be treated with care.

1. I will treat my iPad with care and look after it.

2. I can leave my iPad at school overnight in the year group box.

3. I will never leave my iPad unattended unless in a designated area.

4. I will carry my iPad between lessons as taught by my ICT teacher and will not throw it in the air.

5. I will ensure that my iPad is with me in school each day and that it is charged ready for lessons.

6. I understand that I must have enough space available for the required Apps.

iPad Use Rules

Your iPad is internet enabled and ready for use with Google Classroom, sim cards will not be allowed for use within school. It is a tool for learning only. The ICT department and Deputy Head Pastoral will monitor the internet use of all devices from the office but will also take in iPads to check for misuse from time to time.

1. I will use my iPad in school for school work only.

2. I will use my iPad in the classroom only, unless instructed to by a teacher.

3. I will only use the internet when instructed by a teacher and will only access websites or searches that I have been given permission to view or search.

4. I will not access any games, social media, messaging services or email without permission.

5. If I accidentally access material that I should not or if I see anything I am unhappy with or receive messages I do not like, I will report it to my form or subject teacher immediately.

6. I will respect people's privacy and will not take or share photos or videos without permission.

7. I will not install any Apps, tools or otherwise unauthorised software on the iPad.

8. I understand that access to my iPad may be withdrawn if any of the above rules are broken.

9. On a network, I will only use my own login and password, which I will keep a secret. I will not hack into another pupils' account.

10. I will not look at or delete other people's files.

11. I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.

12. I know that Kenton may check my computer files or iPad and may monitor the Internet sites I visit at any time.

13. I will not upload/share personal photographs/videos of myself, other pupils, members of staff or the Kenton site without approval.

14. I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

15. I will always be polite and respectful when on any social media platform.

16. I will not create a social media account using the Kenton logo.

Pupil's signature:_____ Class:_____ Date:_____

iPad Rules for Junior Pupils

iPad Care Rules

The iPad is for school use only. It is not a toy and should be treated with care.

1. I will treat my iPad with care and look after it.
2. I will return my iPad every day to my class teacher.
3. I will not take my iPad home.
4. I will never leave my iPad unattended unless in a designated area.
5. I will carry my iPad between lessons as taught by my ICT teacher and will not throw it in the air.

iPad Use Rules

Your iPad is internet enabled and ready for use with Google Classroom. It is a tool for learning only. The ICT department will monitor the internet use of all devices from the office but will also take in iPads to check for misuse.

1. I will use my iPad for school work only.
2. I will use my iPad in the classroom only, unless instructed to by a teacher.
3. I will only use the internet, when instructed by a teacher and will only access websites or searches that I have been given permission to view or search.
4. I will not access any social media, messaging services or email without permission.
5. If I accidentally access material that I should not, I will report it to my class or subject teacher immediately.
6. I will respect people's privacy and will not take or share photos or videos without permission.
7. I will not change any security or pass codes.
8. I will not add stickers to my iPad cover or screen.
9. I will not reset my iPad.

Pupil's signature:_____ Class:_____ Date:_____