



Parklands High School

An Academy

Acceptable Use Policy

LEARN RESPECT ASPIRE ACHIEVE



Acceptable Network/Internet Use for Pupils - Parklands High School

Parent Documentation

As part of the school's ICT program we offer pupil's access to the Internet. Before being allowed to use the Internet, all pupils must obtain parental permission and they and their parent(s)/carer(s) must sign and return the enclosed form as evidence of parental/carers approval and their acceptance of the school rules on this matter.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information, resources and opportunities for collaboration, exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

For your information pupils now access our school website, www.parklandsacademy.co.uk to connect to our schools e-learning portfolio. The connection is made via Google Chrome. During some lessons pupils will be asked to log onto this resource with their secure login to either aid them in their studies or to work online. This is a cloud based system and therefore can be used anywhere there is an Internet connection available. Pupils must log into the secure website using their individual username and password which will be provided to them on their first day at school. For further details on this resource please go to: <http://www.realsmart.co.uk/>

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, mobile phones, telephones, movies, games, e-learning, social networking and other media the content of which could be offensive.

We would be grateful if you could read this document in full and complete the permission slip at the end if you wish your child to participate.

Yours sincerely

C Slater - Network Manager



Acceptable Network/Internet Use for Pupils within Parklands High School

Use of the Internet by schools is continuing to grow rapidly. The problems and issues that have been highlighted by the media concern most schools. Whilst some of the media interest is hype, there is real cause for concern and it is imperative that schools consider issues carefully before allowing pupils access, supervised or unsupervised, to the Internet.

It is our belief that there is no present or future technical solution that can completely guarantee the restriction of pupils to unwanted Internet material. Most development work is concentrating on removing access to pornography and even here success is unlikely to be complete. Other areas of unacceptable materials, such as racist, homophobic, extremist, political or violent material is beyond the scope of most safeguarding programs. In these circumstances the initial reaction of a teacher to treat this as an issue for education with parental involvement soon becomes the most sensible course. The development of detailed school policy and practice, together with parent/school contracts in an 'Acceptable Use Policy' is our advised action.

Parklands High School uses an Internet Service which is a filtered broadband connection via a Sophos box. In most cases the filter can be updated immediately should a reason arise. The Internet line is supplied to the school through Virgin Media.

The computer network is owned by the school and is made available to pupils to further their education with activities including research and classroom projects. The school Network/Internet Access Policy has been drawn up to protect all parties – the pupils, staff and the school. The school provides access to its computer network, portals, realsmart accounts, email systems and general connectivity. Pupils are responsible for good behaviour, whether on the school computer network or using their own mobile devices (BYOD) or home connectivity.

All reasonable attempts will be made to protect a pupil's right to privacy and, subject to their strict adherence to the school's acceptable use policy; pupils may enjoy the use of school networks and connectivity to enrich their studies without undue intrusion. This privilege may however be withdrawn without notice at any time. The school reserves the right to examine or delete any files that may be held on the network, email accounts, eLearning accounts, notebooks, pen drives and mobile devices (BYOD) and to investigate and log any Internet sites visited.

This document aims to protect pupils from carrying out activities that may be inappropriate. The school has a duty of care to its pupils and despite the immense educational potential of ICT, there is an unsavoury side to the internet and other current aspects of technology used on mobile devices, which it would be irresponsible to ignore.

In addition, these guidelines extend to ALL information and communication technology devices, including privately owned *3G mobile phones, iPhones, Androids, iPods, iPads, PDAs, 'Blackberry-type' devices, USBs, External hard drives, CDs, DVDs, Social networking sites (e.g. Facebook, Flickr & Twitter) and also including our e-learning site (Realsmart)*

School Policy

The school encourages use by pupils of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our pupils will be entering.

Online services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the pupils. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by pupils.

All pupils will be informed by staff of their rights and responsibilities as users early on in Year 7 either as an individual user or as a member of a class or group.

Where possible, the school's chosen information provider has organised information resources in ways that point pupils to those sites that have been reviewed and evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated, pupils will be provided with guidelines and lists of resources particularly suited to the learning objectives of each specific area. Pupils may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to all pupils, and kept under constant review.

General guidelines for Internet use;

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.

Pupils are responsible for ALL work done via their own user areas, this includes Internet browsing. It is imperative that pupils DO NOT allow any other user on their user area or give their passwords to any other pupil.

The Internet is provided for pupils to conduct research and communicate with others. Parent(s)/carer permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Network/Internet are responsible for their behavior and communications over the network. It is presumed that users will comply with school standards and will honor the agreements they have signed.

Computer storage areas, Realsmart, USB drives, mobile devices and phone/memory cards will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers, Realsmart, external drives, mobile devices or disks will be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources as mentioned previously in this document.

Items to note:

- Access to Parklands High School network, Realsmart etc. is a privilege, not a right: access entails responsibility and inappropriate use will mean loss of access.
- Pupils are responsible for the integrity of their digital devices. It is a condition of bringing mobile devices into school that the owner accepts full responsibility for everything done using it and its connectivity. Any mobile devices being used to access the school network must be seen and logged by the network manager before use. Photographs should only be taken with the agreement of all parties, these should be deleted off any shared resource and downloaded into pupils own user area.
- Pupils are responsible for the security of their password, the integrity of their network area and the appropriate use of privately owned communication devices; they must keep their password secret. Pupils must not use another person's password or trespass in another person's folders, work or files.
- Pupils must never open/send or display offensive material.
- It is not acceptable for pupils to use obscene language either verbally or written.
- Pupils must not damage computers/monitors/printers or the computer network; hack, vandalise, damage or disable the personal or intellectual property of another person or the school.
- Pupils must not pirate software, or copy software/school property onto mobile devices, distribute already pirated software, compromise school licensing, debilitate or disable computers, systems or networks through the misuse or overuse of electronic distribution or the spreading of computer viruses through the inappropriate use of files, CD/DVDs, USBs, PSPs, iPods, iPhones, Mobile devices or other mass storage devices.
- Pupils must not place any unauthorised applications on the school network; if in doubt see the network manager.
- Pupils must not compromise the security or integrity of any ICT systems, whether from inside or outside the school and whether that system is owned by the school or by other organisations or individuals.
- School computer and internet use should be appropriate to a pupil's education. Under no circumstances must pupils attempt to hack, crack or otherwise circumvent the school filter (e.g. by the installation of other browsers or plug-ins such as Mozilla Firefox) it is against school rules for any pupil to have any proxy bypass applications on any device or to download and use them on the network, this will be seen as a serious breach of school agreements and could lead to permanent exclusion from the Internet.
- Pupils must not transmit, re-transmit, distribute, publish, promote, market, or store material on or through the school network or the internet, which is threatening, abusive, hateful, obscene, indecent, or defamatory or involves or encourages conduct that may constitute a criminal offence.
- Pupils are responsible for email sent via their personal and school account. Emails should be written carefully and politely; pupils cannot expect that email messages will always be private. The email service given through school can be revoked at any time.
- The use of computer 'chat' or 'messaging' over the school network in any form is not allowed without the express permission of a teacher for specific academic purpose.
- Pupils must not use camera/video facilities in mobile devices to photograph other members of the school community without their express permission for a justifiable educational objective. They must under no circumstances post image/video files (or links to such files) of other members of the school community via the internet without the members permission (via YouTube, Facebook, Twitter etc.)
- Pupils must never violate copyright laws
- Pupils must never use other user's passwords and user accounts.
- Pupils must never intentionally waste limited resources. (ie: paper for printing)

- Pupils must never download upgrades to network resources, games or run any executable files
- Accessing social networking sites via proxy server blockers is a serious breach of this contract
- Playing games with the exception of educational games under teacher/member of staffs' supervision is not allowed.

Handheld and Mobile Devices

Handhelds and mobiles (BYOD), including Blackberries, iPhones, iPads etc. are at high risk from theft due to their size and nature of usage. The school accepts no liability for misuse, loss or damage. Pupils who bring these devices into school do so at their own risk and are responsible for their safekeeping. Pupils should take care to keep these devices concealed when not in use and to be conscious of onlookers who may be targeting devices for theft. In the event that a device is stolen, pupils will be expected to report the theft to the police, obtain an incident number and inform the Network Manager ASAP. You must also report the theft to the relevant device provider who will stop the system use. Users of mobile devices must inform the Network Manager of devices being used on the network and to access the internet, a log will be made of the device for school records. The internet connection must be set up by a member of the IT technical support team.

Network Access

Passwords protect the network from access by unauthorised people, including outside agencies. Therefore never give your network password to anyone else. Any activity on the network done on your user area or with your username/password will be your responsibility. You should ensure that you change your passwords every term.

The school does not allow the connection of non-school equipment to the network without the knowledge of the Network Manager.

Electronic Mail (e-mail)

The school email system is provided through Realsmart using Gmail. Email messages must be treated like any other formal written communication. Messages cannot be considered to be private, secure or temporary. Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone. Improper statements in email can give rise to personal liability and liability for the school can constitute a serious disciplinary matter. Emails that embarrass misrepresent or convey an unjust or unfavourable impression of the school, employees, pupils, suppliers and other schools are not permitted. Do not create or send email messages that are defamatory. Defamatory emails whether internal or external can constitute a published libel and are actionable. Never send confidential or sensitive information via email unless using encryption software. Do not create or send email messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject another pupil or member of staff to public humiliation or ridicule; this is equally true via email. Do not use email to transmit or circulate copyrighted materials. No spamming using either your school or personal email should be sent in respect of Parklands High School or relating to any member of the school community, it will not be tolerated and it will lead to immediate loss of your school email and may result in further action being taken. (Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam))

Privacy; email messages to or from you cannot be considered to be private or confidential. Although the school has no policy to routinely examine the content of individuals email, the school reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfill legislations, respond to allegations of wrongdoing, detect pupil wrongdoing, protect the rights or property of the school, protect IT system security or to comply with legal process. It is not permissible to access or to send email from another person's account either directly or indirectly.



Facebook – Advice for Privacy Settings

When an account is first created on Facebook, the content within the Facebook account is automatically made public to everyone. Therefore it is vital that the settings are changed to ensure your information on Facebook is only available to the people you want it to be available to!

It is up to the pupil and parents to check that the highest possible settings are accepted on any social network site. This is for the benefit of all concerned.

Although devices, forms of cyber bullying, internet and social networking sites specified in this policy are referred to by brand name for quickness of communication and ease of understanding, the policy should be understood as being agnostic with regard to brand and applicable to equivalent devices, social networking sites, websites or forms of bullying regardless of manufacturer, internet service provider or minor variation in bullying strategy.

Social networking sites such as facebook are not allowed to be used within school at this present time.



Years 9, 10 & 11 only - Some members of staff have lesson support groups etc. on twitter. Members of staff may invite you to join one of these groups if it is relevant to your learning. You may follow one of these groups if:

- You have been invited by a member of staff to do so
- You are accepted on to a member of staff or group account by the relevant member of staff
- You have read, understand and agree to the twitter agreement policy when setting up your account
- You have no unacceptable or inappropriate information/images/photographs on your twitter account and your twitter account name has reference to your birth name

No pupils in year 7 & 8 will be allowed access to school twitter accounts.

It is not acceptable to use social networking sites during the school day or on school premises.



Years 9, 10 & 11 only – Vimeo can be used within school by departments as a form of assessment. You may be asked to log into the site to review or comment on videos which will be uploaded by members of your group or staff. If you have any concerns about your child using Vimeo or appearing in any school related videos on this site please contact the school. To review Vimeo please go to: <https://vimeo.com/>. By signing the AUP you are agreeing to your child using this form of assessment.

The above media is only a sample of current available media. If age restrictions are clear on any media site your child is asked to use within school they will be made aware of it. All media sites come with terms and conditions that should be read alongside this document. If you have any concerns please do not hesitate to contact the school.



Children and young people are likely to be equally or more advanced internet users than some parents/carers. However, being proficient in technology does not mean they have the life-experience and wisdom to handle all of the situations they encounter.

Children and young people are prone to the same kinds of risks (including spam and scam emails, fraud and identity theft) as everybody else. However, there are also other, more sinister threats that may result from going online, such as inappropriate contact from people who may wish to abuse, exploit or bully them, the exposure to inappropriate material.

If you look after children either as a parent, carer, teacher or other responsible adult it is essential that you are up to date with current internet trends and risks. (Information taken from 'Get Safe Online'- www.getsafeonline.org)

Responsibility for e-safety depends on schools, staff, governors, parents and the pupils themselves taking responsibility for their actions online.

The school provides additional e-safety information for pupils during specific lessons on the school timetable and provides a link to important information and updates via the pupils cloud resource (Realsmart). Information is also available via the school website; www.parklandsacademy.co.uk under the students and parents tabs. There is also information available from our eSafety Bulletin Board which is at the end of the concourse.

All teaching staff in school receive ongoing training and information regarding eSafety, if you have any questions please do not hesitate to ask. You will also receive information regarding eSafety during your SECURE lessons.

To report an eSafety concern or issue you should, in the first instance speak to a member of staff in school immediately. If you wish to report the incident online you can do this by going to www.parklandsacademy.co.uk/students/E-Safety and Responsible Social Networking/Report an eSafety Issue when filling in the form please ensure you put as much information as possible. If you do not wish to report your issue online there is a Pupil Concern Box available in the LRC for you to 'post' any concerns you may have, again when writing your concerns please put as much information as possible. It is useful for us to have your name and registration form details on any forms you complete but this isn't essential. If you wish to remain anonymous this is fine, it is better to report your concern anonymously than to not report it at all. To report an incident to an outside agency please go to: <https://www.ceop.police.uk/Ceop-Report/> The CEOP site is full of useful information, help and support.

The following document will be sent home for all new pupils to Parklands and should be read in conjunction with the above. Once both parties are happy that they have read all the information in the full policy and summary and understood the contents the form below should be signed and returned.



Parklands High School, An Academy - Acceptable Network/Internet Use for Pupils

Information for Parents/Carers

As part of the school's ICT program we offer pupils access to the school network and the Internet. Before being allowed to use the Internet, all pupils must obtain parental permission and they and their parent(s)/carer(s) must sign and return the form attached as evidence of parental/carer approval and their acceptance of the school rules on this matter.

The information attached is in the form of bullet points. This form should be read in conjunction with the full policy that is available on our school website: www.parklandsacademy.co.uk/Students/AUP.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information, resources and opportunities for collaboration, exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

For your information pupils now access our school website, www.parklandsacademy.co.uk to connect to our school's e-learning portfolio. The connection is made via Google Chrome. During some lessons pupils will be asked to log onto this resource with their secure login to either aid them in their studies or to work online. This is a cloud based system and therefore can be used anywhere there is an Internet connection available. Pupils must log into the secure website using their individual username and password which will be provided to them on their first day at school. For further details on this resource please go to: <http://www.realsmart.co.uk/>

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, mobile phones, telephones, movies, games, e-learning, social networking and other media the content of which could be offensive.

We would be grateful if you could read this document alongside the full AUP online and complete the permission slip attached if you wish your child to participate.

Yours sincerely

C Slater - Network Manager

This document should be read in conjunction with the full AUP available on our website and once the information is read and understood the enclosed return sheet should be returned to: Ms C Slater, Network Manager or your Form Tutor

For Pupils:

- I will only use school Internet and IT facilities for educational purposes which follow the teachers' instructions. This includes email, video, messaging, social media (Twitter), Internet, file-saving and printing.
- I will only use my mobile phone or mobile device in school when permission has been granted by a teacher. If permission is granted, I will use my mobile device as if it was a school computer, following all the rules for using school computers.
- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to.
- I will, at the request of the Headteacher or Network Manager, share any resources that are on the school network with them.
- I will only use my school-supplied email address for school-related activities and will not send out spam/junk email. Group email is not permitted unless authorised by a teacher.
- I will not look at or delete other people's work or files.
- I will not log on to any school related sites or the network as any other user, even if they have given their permission for me to.
- I will keep up to date with eSafety issues by regularly looking at information shared via Realsmart, the school bulletin and the information board on the concourse. I will report any eSafety concerns either via the online form available on Realsmart, by using the Pupil Concerns Box available in the LRC or by telling any member of staff in school.
- I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils or teachers.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I will not look for or look at unpleasant or sociably unacceptable websites in school. I will inform a member of staff if I think a website might be unsuitable.
- I will not give out my personal details, such as my name, address, school or phone number on the Internet.
- I will not meet people I've met on the Internet unless I have told my parents and they come with me.
- I will not upload or download any pictures, writing or films which might upset people online.
- I will not write potentially libelous comments online about pupils, staff or the school.
- I will treat all IT equipment at school with respect and ensure the computer is left in the state that I found it.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a member of staff is concerned about my online safety or my behaviour when using school computers. Any work on the network or any online activity should not be deemed as 'personal' and can be viewed by the Headteacher or Network Manager if needed.
- I will respect copyright when making use of images and videos in my school and home work.
- I will not look for, view, upload or download offensive, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a member of staff immediately.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy and the person in the pictures permission. Images will only be used on the Internet or in the media with permission. No images should be posted on any social network sites.
- I will not look for ways to bypass the school filtering or proxy service.
- Access to Parklands High School network, Realsmart and any other school related package is a privilege, not a right: access entails responsibility and inappropriate use will mean loss of access.
- Pupils must not compromise the security or integrity of any ICT systems, whether from inside or outside the school and whether that system is owned by the school or by other organisations or individuals.

This document should be read in conjunction with the full AUP available on our website and once the information is read and understood the enclosed return sheet should be returned to: Ms C Slater, Network Manager or your Form Tutor



Acceptable Network/Internet Use for Pupils - Parklands High School

I understand that these rules are designed to keep me/my child safe and that if they are not followed, sanctions may be applied and parents/carers may be contacted. Any breach of the enclosed will result in a sanction being imposed which includes permanent exclusion from the school. The school will be the final arbiter of any sanction imposed.

Parental/Carer Agreement slip
(Must be completed by both pupil and a parent/carers)

Name of Pupil
please use capital letters and clearly write your name:

.....

Form

.....

As a school user of the Network and Internet I agree to comply with the school rules on its use. I will use the network and Internet in a responsible way and observe all the restrictions explained to me both verbally and in this document.

Pupil SignatureDate

As the parent/carers of the pupil signing above, I grant permission for my son/daughter to use the school network and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

Parent/Carer SignatureDate

This document should be read in conjunction with the full AUP available on our website and once the information is read and understood the enclosed return sheet should be returned to: Ms C Slater, Network Manager or your Form Tutor