



Secondary Network, e-Safety & Internet Acceptable Use Policy

Policy objectives	3
Key roles and responsibilities	4
Education & Training - e-Safety	6
Use of the School Network and the Internet	8
Use of digital and video images	8
Acceptable use of AI tools	15
School Actions & Sanctions	16
Student/Pupil Acceptable Use Agreement	22
B.O.Y.M Agreement	28

Policy objectives

- To ensure the safety of users (staff and students) of the school network and internet.
- To ensure the responsible use of the school network and internet by users.
- To ensure users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- To ensure that users are protected from potential risk in their use of technology in their everyday work in school.
- To ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner.

Rationale/key principles

The use of exciting and innovative tools relating to Internet and ICT use in school and at home has been shown to raise educational standards and promote pupil/student achievement. However, the use of these new technologies can put young people at risk within and outside the School.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other school policies (e.g, Positive Behaviour, and Child Protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope

The policy applies to all members of the school community, including **staff, students, parents and visitors** who use the school's network and internet facilities and sets down the standards which users are required to observe in use of the school's ICT equipment and network.

It is the responsibility of **ALL** users to familiarise themselves and comply with this policy.

The school will deal with incidents within the scope of this policy (and associated behaviour and anti-bullying policies) occurring during school hours and utilising school technology. Incidents of which we become aware happening outside this remit will be reported to parents and may be

reported to outside agencies where appropriate.

The following usage policy is designed to help staff and pupils understand the expectations for the proper use of the computing facilities and use the resources it provides. The policy is designed to protect pupils, staff and the school.

Key roles and responsibilities

The ICT Coordinator and the IT Systems Manager are responsible for the development of this policy in consultation with the Secondary Leadership Team and Managing Board/advisory committees for Safeguarding, Child Protection & Pastoral Care, and Premises, Environment, Health and Safety.

Managing Board/Advisory committees:

The Managing Board, in consultation with the advisory committee members for Child Protection, Safeguarding & Pastoral Care, and Premises, Environment, Health and Safety are responsible for:

- the approval of the Network and Internet Acceptable Use Policy and for reviewing the effectiveness of the Policy.
- ensuring filtering and monitoring standards are met.

Senior Management Team

The Senior Management Team are responsible for:

- Buying-in the filtering and monitoring system used by the school
- Documenting what is blocked or allowed, and why
- Reviewing the effectiveness of provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded
- Overseeing reports
- Making sure staff:
 - Understand their role
 - Are trained appropriately
 - Follow policies, processes and procedures
 - Act on reports and concerns

ICT Coordinator:

- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place;
- provides training and advice for staff;
- liaises with school ICT technical staff;
- reports regularly to the Secondary Leadership Team.

IT Systems Manager:

Is responsible for ensuring that the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack;

- that the school meets the e-Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant e-Safety legislation and guidance.
- that users only access the school's networks through a properly enforced Password Protection Policy, in which passwords are regularly changed.
- that he/she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant.
- that the use of the network/Internet/email is regularly monitored in order that any misuse/attempted misuse can be reported to the The ICT Coordinator for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.

Designated Safeguarding Lead / Deputy-DSL

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

Is responsible for

- Checking relevant reports
- Responding to safeguarding concerns identified by filtering and monitoring
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

Teaching and Support Staff:

- are responsible for ensuring that they have an up to date awareness of e-Safety matters and of the current school e-Safety Policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy (See Appendix).
- they report any suspected misuse or problem to the The ICT Coordinator for investigation/action/sanction.
- digital communications with pupils/students (email/Virtual Learning Environment (VLE)/voice) are on a professional level and only carried out using official school systems.
- e-Safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils/students understand and follow the school e-Safety and Acceptable Use Policy.

- they are aware of e-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

Students

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will sign before being given access to School systems (see appendix);
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
- know and understand school policies on the taking/use of images and on cyberbullying.
- will understand the importance of adopting good e-Safety practice at all times and remain compliant with the expectations identified in the Student Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)
- endorsing (by signature) the Student Network, e-Safety and Acceptable Use of ICT Policy

Education & Training - e-Safety

Staff

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

- In-house training sessions on the topic of e-Safety and a requirement to qualify in this area by completing a study programme as part of CPD over the period of six-months. This cycle applies to existing as well as newly appointed staff.
- All new staff will receive the e-Safety policy as part of their induction programme, ensuring that they fully understand the school e-Safety and Acceptable Use Policies.
- The The ICT Coordinator (or other nominated person) will ensure that they remain as up to date as possible regarding issues and technologies that may affect the school's Network, e-Safety and Internet Acceptable Use policy and appropriate response.

Students

The education of students in e-Safety is an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience. e-Safety education will be provided in the following ways:

- A planned e-Safety programme will be provided as part of ICT/PSHEE lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Rules for use of ICT systems/internet will be posted in all rooms and displayed on log-on screens.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Parents

Training is offered to parents as:

- An informative resource (booklet/online) containing guidance and links to agencies that support and promote e-Safety
- Regular information for parents provided in the Secondary Updates and if needed parent forums can take place with training and discussions.

Use of the School Network and the Internet

Use of the school network and the Internet by all school staff and students is permitted and encouraged where the use is suitable for educational purposes.

Acceptable use of the network and Internet is characterised when students use the facilities to further their education and when staff ensure that the computer equipment and the Internet may only be used for legal activity consistent with the aims, objectives and rules of the school. This will include professional activities such as teaching, research, administration and management.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches

for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg. on social networking sites.
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act, the Czech Act on Personal Data - Act No. 101/2000 Coll. and Directive 95/46/EC). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents or carers is obtained via an electronic form every 3 years (or when a student joins Park Lane) before photographs of students / pupils are published on the school website
- Student's work can only be published with the permission of the student and parents or carers

Personal data will be recorded, processed, transferred and made available according to the UK Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that

- 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- It has a Data Protection Policy
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they

- At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Students KS3			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons		X	X				X	
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones / cameras				X				X
Use of other mobile devices eg. tablets, gaming devices		X					X	
Use of personal email addresses in school, or on school network			X					X
Use of school email for personal emails			X					X
Use of messaging apps		X					X	
Use of social media				X				X
Use of blogs	X						X	

Communication Technologies	Students KS4				Students KS5			
	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons			X				X	
Use of mobile phones in social time	X - courtyard only				X			

Taking photos on personal mobile phones / cameras				X				X
Use of other mobile devices eg. tablets, gaming devices			X				X	
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps			X				X	
Use of social media				X				X
Use of blogs			X				X	

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 the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) 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.
- Students should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate

communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

Unsuitable / inappropriate activities

Some internet activity eg. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities eg. cyber-bullying is 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 school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children.					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character)					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
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				X		
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large				X		

files that hinders others in their use of the internet)			
On-line gaming (educational)	X		
On-line gaming (non educational)			X
On-line gambling			X
On-line shopping / commerce			X
File sharing		X	
Use of social media			X
Use of messaging apps			X
Use of video broadcasting eg Youtube		X	

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should**

be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Acceptable use of AI tools :

Acceptable Use of AI Tools	<ul style="list-style-type: none"> - In general AI tools may be used for educational purposes. - Use of AI requires staff approval for certain projects or age groups.
Ethics and Responsible Use	<ul style="list-style-type: none"> - All assignments must be the student's original work; use of AI for completing assignments is subject to review. - If AI is used for research or writing assistance, students must disclose its use.
Privacy and Data Protection	<ul style="list-style-type: none"> - AI tools may not collect or store personal information about students unless explicitly approved. - Ensure AI tool compliance with GDPR/FERPA for any collected data.
e-Safety and Monitoring	<ul style="list-style-type: none"> - AI use will be monitored to ensure appropriateness and prevent access to harmful content. - Students should critically evaluate AI-generated content and verify information.
Training and Support	<ul style="list-style-type: none"> - Staff will receive training on guiding responsible student use of AI. - Students will learn about AI ethics and reliability in digital citizenship classes.
Disciplinary Measures for Misuse	<ul style="list-style-type: none"> - Misuse of AI for plagiarism or inappropriate

	content generation will lead to disciplinary action. - Consequences will range from warnings to more severe penalties, based on the infraction. *Academic Honesty Policy addresses this issue
--	---

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. 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 normal behaviour / disciplinary procedures as follows:

Students: Actions / Sanctions

	Refer to tutor / HOY	Refer to Subject leader	Refer to Deputy Head / Head of of Secondary	Refer to police	Refer to IT Systems Manager	Inform parents / carers	Removal of Internet / network access rights	Verbal or written warning	Further sanction Eg. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons		X			X				
Unauthorised use of mobile phone / digital camera / other mobile device	X	X				X			
Unauthorised use of social media / messaging apps / personal email	X								
Unauthorised downloading or uploading of files	X				X		X		
Allowing others to access school network by sharing username and passwords	X								
Attempting to access or accessing the school network, using another student's account	X		X		X	X		X	X

Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X	X	X
Corrupting or destroying the data of other users	X		X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions			X						X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						X
Using proxy sites or other means to subvert the school's filtering system					X				X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X				X
Deliberately accessing or trying to access offensive or pornographic material			X		X				X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X				X

Staff:

Actions / Sanctions

	Refer to line manager	Refer to Deputy Head / Head or or Secondary	Refer to police	Refer to IT Systems manager (filtering/security)	Verbal or written warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X			X		
Unauthorised downloading or uploading of files	X			X	X		
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	X	X		X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X			X			
Deliberate actions to breach data protection or network security rules	X	X		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X	X	X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X	X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X			X		
Actions which could compromise the staff member's professional standing	X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system		X		X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X			
Continued infringements of the above, following previous warnings or sanctions						X	X

Appendices

Student/Pupil Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement and the Behaviour Policy, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school/academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the student acceptable use agreement to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student/Pupil:

Group/Class:

Signed:

Date:

Parent/Carer Countersignature

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become

aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I

- am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Managing Board and in the event of illegal activities the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Park Lane International School “Bring Your Own MacBook” (B.Y.O.M.) Responsible Use Guidelines

Purpose:

The school uses instructional technology as one way of enhancing our mission to teach the skills, knowledge and behaviours students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills, the school operates a B.Y.O.M. policy where either school borrowed or purchased MacBook can access our network during the school day within school premises. A complete set of user responsibilities is stated in the Acceptable Use Policy and the attached guidelines regarding B.Y.O.M. stated in the body of this policy document.

Park Lane International School strives to provide appropriate and adequate technology to support instructional purposes. The use of MacBooks by students is a core component of this approach because it supports the educational experience where a common device can be managed and common software installed that is the best fit for our curriculum. In effect, all students participate in the B.Y.O.M. policy by having access to their own MacBook.

The associated investment in a MacBook, for private purchase, should be considered as an investment for the years of formal education. MacBooks are robust and with reasonable treatment will last for six years. Therefore, this is not a B.Y.O.D. policy because it focuses on MacBooks as the common device in school. Other digital devices are prohibited from use on the premises. The only exception being direct permission granted by the Principal.

An important component of B.Y.O.M will be education about appropriate online behaviours. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviours. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using their MacBook. The use of technology is not a necessity but a privilege. When abused, privileges will have to be reviewed on an individual case basis.

The B.O.Y.M. policy refers to the use of a personally issued or bought MacBook. Under teacher or learning centre direction it can extend to the use of iPads, eBook readers and exceptions in specific subjects, such as the possible use of Raspberry Pi, Arduino or Micro Bits in Computer Science.

Guidelines:

- Students and parents/guardians participating in B.Y.O.M. must adhere to the Student Code of Conduct, Student Handbook, Acceptable Use Policy and all Board Policies, particularly Internet Acceptable Use.
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects. Some subjects might require the download and installation of software where the administrator password (if not known to the student) will

need to be applied by their parent/guardian.

- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- During school hours,, devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes (such as making personal calls or video calls, text messaging/chat, social media, downloading movies and music or software not prescribed in class).
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
- During school hours, devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.

Students and Parents/Guardians acknowledge that:

- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- Park Lane International School is authorised to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection.
- Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct. If the device is locked or password protected the student will be required to unlock the device at the request of a school administrator
- Personal devices must be charged prior to school and run on battery power while at school.

Lost, Stolen, or Damaged Devices:

Each user is responsible for his/her own device and should use it responsibly and appropriately. Park Lane International School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

Network Considerations:

Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the 'Park Lane' wireless network to access the internet. The school does not guarantee connectivity or the quality of the connection with personal devices. Although help may be offered, Park Lane International School is not responsible for setting up or maintaining MacBooks.

B.O.Y.M Agreement:

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as possible disciplinary action. During the course of the school year, additional rules regarding the use of personal devices may be added.

Name:

Signed:

Date: