IT Acceptable Use Policy

1. Introduction

1.1 The School is committed to protecting its Governors, staff, parents, students, volunteers and associated third parties, (known as the School Community), from illegal or damaging use of technology by individuals, either knowingly or unknowingly.

1.2 As users of the School's IT services individuals have a right to use its computing services; that places responsibility on these users which are outlined below. Misuse of technology in a way that constitutes a breach or disregard of the following policy may also be in breach of other School policies.

1.3 Ignorance of this policy and the responsibilities it places on users is not an excuse in any situation where it is assessed there has been a breach of the policy and its requirements.

1.4 Individuals who connect their own IT equipment to the School's network and the services available (including the use of 3G and 4G) are particularly reminded that such use requires compliance to this policy.

1.5 Individuals are directed to this policy during their induction and are required to acknowledge their agreed adherence to and compliance with the policy when they first log on to the network.

1.6 A copy of this policy is available on request and on the school website. In the case of students, the School encourages the participation of parents to help the School safeguard their welfare and promote the safe use of technology.

2. Purpose

2.1 The purpose of this policy is to:

2.1.1 outline the acceptable and unacceptable use of technology including "online services", owned or operated by the School or by a school approved third-party, and acceptable or unacceptable general behaviour in IT areas;

2.1.2 educate and encourage individuals to make good use of the business and educational opportunities presented by access to technology;

2.1.3 safeguard and promote the welfare of the School Community, by anticipating and preventing the risks arising from:

2.1.3.1 exposure to harmful or inappropriate material (such as, (but not limited to), pornographic, racist, extremist or offensive materials);

2.1.3.2 the sharing of personal data, including images;

2.1.3.3 inappropriate online contact or conduct; and

2.1.3.4 cyberbullying and other forms of abuse;

2.1.4 help individuals take responsibility for their own safe use of technology (e.g. limiting the risks that individuals are exposed to when using technology);

2.1.5 ensure that the School Community use technology safely and securely and are aware of both external and peer to peer risks when using technology.

2.2 These rules are in place to protect the School Community. Inappropriate use exposes the School and its associated third-party partners to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

3.1 This policy applies to all the School Community at Leighton Park School as outlined in 1.1.

3.2 The School will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including, (but not limited to):

3.2.1 the internet

3.2.2 email

3.2.3 mobile phones and smartphones including wearable technology

3.2.4 desktops, laptops, netbooks, tablets / phablets

3.2.5 personal music players

3.2.6 devices with the capability for recording and / or storing still or moving images

3.2.7 social networking, micro blogging and other interactive web sites

3.2.8 instant messaging, (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards

3.2.9 webcams, video hosting sites, (such as YouTube)

3.2.10 gaming sites

3.2.11 Virtual Learning Environments

3.2.12 Interactive Boards / Screens

3.2.13 other photographic or electronic equipment e.g. GoPro devices and other wearable technology.

3.3 This policy also applies to the use of technology on and off school premises if the use involves any member of the School Community or where the culture or reputation of the School or member of staff are put at risk.

4. Safe use of technology

4.1 We want the whole School Community to enjoy using technology and to become skilled users of technology. We recognise that this is crucial for organisational efficiency, career progression and further education.

4.2 The School will support individuals to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of the School Community and the security of our systems. The School Community are educated about the importance of safe and responsible use of technology, to help protect themselves and others online.

4.3 Students may find the following resources helpful in keeping themselves safe online:

http://www.thinkuknow.co.uk

http://www.childnet.com

http://www.childline.org.uk

4.4 Staff are encouraged to speak with the IT team or Director of IT should they require advice on keeping themselves safe online.

5. Procedures

5.1 Individuals are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If an individual is aware of misuse by others, he / she should talk to a member of staff or Senior Manager about it as soon as possible.

5.2 Any misuse of technology by students will be dealt with under the School's Behaviour and Discipline Policy. Any misuse by staff will be dealt with under the School's Disciplinary Procedures. Any misuse by other members of the School Community may be dealt with through the relevant School policies or legal procedures.

5.3 Individuals must not use their own / School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying policy. If a person thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a member of staff or Head of Department about it as soon as possible. See the School's Anti-Bullying policy for further information about cyberbullying and online safety, including useful resources.

5.4 For all other members of the School Community not detailed in 5.3, they must not use their own, or the School's technologies to harass, victimise or bully others. Any instances will be dealt with through the Staff Code of Conduct and the Disciplinary Policy, Staff.

5.4 In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures, (see the School's Safeguarding & Child Protection Policy). If an individual is worried about something that he / she has seen on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a member of staff about it as soon as possible.

5.5 In a case where a student is considered vulnerable to radicalisation, they may be referred to the Channel programme / Prevent. Channel and Prevent focus on support at an early stage for people who are identified as being vulnerable to being drawn into terrorism.

5.6 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the Director of IT who will record the matter centrally.

6. Unacceptable Usage

6.1 The School provides internet access and an email system to students to support their academic progress and development.

6.2 Unacceptable use of School technology and network resources may be summarised as, but not restricted to:

6.2.1 Actions which cause physical damage to any IT hardware, including peripherals (eg, mouse, cables, wiring, printers);

6.2.2 Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;

6.2.3 Viewing, retrieving, downloading or sharing any offensive material (or attempting to do such) which may include content that is abusive, racist, considered to be of an extreme or terrorist related nature, violent, depicting cruelty to animals, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity;

6.2.4 Threatening, intimidating or harassing staff, students or others;

6.2.5 Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;

6.2.6 Defamation;

6.2.7 Unsolicited advertising often referred to as "spamming";

6.2.8 Sending emails that purport to come from an individual other than the person sending the message using, e.g., a forged address;

6.2.9 Not adhering to the acceptable data storage levels set by the Director of IT;

6.2.10 Attempts to break into or damage computer systems or data held thereon;

6.2.11 Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, eg use of equipment which is inadequately protected against viruses and spyware;

6.2.12 Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;

6.2.13 Using the School network for unauthenticated access;

6.2.14 Any other conduct which may discredit or harm the School, its staff, community or the IT facilities;

6.2.15 Using the IT facilities for gambling;

6.2.16 Using the IT facilities for carrying out any illegal trading activity.

6.3 This policy sets out the following rules and principles with which the School Community must comply:

6.3.1 Authorisation - access and security

6.3.2 Use of the internet and email

6.3.3 Use of mobile electronic devices and

6.3.4 Photographs and images. These principles and rules apply to all use of technology.

6.4 Anyone who mistakenly accesses inappropriate material should notify IT Support.

6.5 The School may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

7. Sanctions

7.1 Where an individual breach any of the School rules, practices or procedures set out in this policy or the appendices, the School may apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour and Discipline and Staff Code of Conduct policies. Any action taken will depend on the seriousness of the offence.

7.2 Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy, Behaviour and Discipline policy and Staff Code of Conduct policy.

Key Principles and Rules

8. Authorisation - access and security

8.1 In order to use the School's IT Facilities individuals must first be properly registered to use such services. Registration to use School services implies and is conditional upon acceptance of this Acceptable Use Policy.

8.2 The registration procedure grants authorisation to use the core IT Facilities of the School. Following registration, a username and password will be allocated to each member of the School Community, (where required). Authorisation for other services may be requested by application to the School IT Helpdesk. (itsupport@leightonpark.com)

8.3 Any attempt to access or use any user account or email address, for which the person is not authorised, is prohibited.

8.4 Individuals may not use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by a member of staff or SLT.

8.5 Individuals must take all reasonable precautions to protect the School's resources (including the IT facilities and the School's information and data), their username and passwords.

8.6 Purpose of Use

8.6.1 IT facilities are provided primarily to facilitate a person's essential work. Use for other purposes, such as personal email or recreational use of the Internet, is only permitted during the permitted times specified by the School and is a privilege, which can be withdrawn at any time and without notice. Any such use must not interfere with a student's studies or a staff members responsibilities or any other person's use of computer systems and must not, in any way, bring the School into disrepute.

8.6.2 School email addresses and associated School email systems must be used for all official School business. All individuals must regularly read their School email and delete unwanted or unnecessary emails at regular intervals.

8.7 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of staff and students. The School Community must not try to bypass this filter on any device including their own.

8.8 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If anyone thinks or suspects that an attachment, or other downloadable material, might contain a virus, he / she must speak to a member of IT Support staff before opening the attachment or downloading the material. Individuals must not disable or uninstall anti-virus software on the School's computers.

8.9 Privacy and Monitoring

8.9.1 All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. The School Community are personally responsible and accountable for all activities carried out under their username. The password associated with a personal username must not be divulged to any other person.

8.9.2 Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.

8.9.3 For the protection of the School Community, use of email and of the internet when accessed via the School network will be monitored by the School. Individuals should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Individuals should not assume that files stored on servers or storage media are always private

8.9.4 Individuals must not interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, individuals must not make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

9 Use of the internet and email

9.1 The School does not undertake to provide continuous Internet access. Email and website addresses at the School may change from time to time.

9.2 Use of the internet

9.2.1 Individuals must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently

9.2.2 Individuals must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Individuals must tell a member of staff or line manager immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

9.2.3 Students must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons. This would only be authorised by SLT.

9.2.4 Individuals must not bring the School into disrepute through their use of the internet.

9.2.5 Copyright Compliance

9.2.5.1 Individuals must abide by laws relating to the use and protection of copyright.

9.2.5.2 Individuals must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose eg research, then copyright permission must be obtained and documented before such material is used.

9.2.5.3 Individuals are reminded that the School treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

9.3 Use of email

9.3.1 Students must use their School email accounts for any email communication with staff. Communication either from a personal email account or to a member of staff's personal email account is not permitted. Equally, Staff must use their School email accounts for any email communication with students.

9.3.2 Email should be treated in the same way as any other form of written communication. Individuals should not include or ask to receive anything in an email which is not appropriate to be published generally or which they believe the School, or their parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone they did not intend.

9.3.3 Individuals must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If they are unsure about the content of a message, they must speak to a member of staff. If they come across such material, they must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

9.3.4 Trivial messages and jokes should not be sent or forwarded through the School's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the School's network to suffer delays and / or damage.

9.3.5 Individuals must not read anyone else's emails without their consent.

10 Use of mobile electronic devices

10.1 "Mobile electronic devices" includes but is not limited to mobile 'phones, smartphones, tablets, laptops and MP3 players or any wearable technology.

10.2 Students in Y7 to 11 are not permitted to have their phone with them during the school day. Mobile phones should be stored securely in the lockable space provided. Students found with their phone or found using their phone between 0800 to 1730 will have the device confiscated and returned at the end of the day. A detention will then be served.

10.3 Individuals who are permitted to use their mobile electronic devices may use their devices on the “LPS Wireless” Wi-Fi network only. Students are not permitted at any time to connect devices with a network cable in any part of the School or to any other school Wi-Fi network.

10.4 Students must not communicate with a member of staff’s personal (as opposed to School) mobile phone except when this is expressly permitted by a member of staff (e.g. if staff member has no school mobile and communication is required for the normal running of School business). For example, this may on occasion be necessary during an educational visit. Any such permitted communications should be brief and courteous.

10.5 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether they are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying policy and Behaviour & Discipline policy), the School's safeguarding procedures will be followed in appropriate circumstances (see the School's Child Protection and Safeguarding policy and procedures).

10.6 Mobile electronic devices may be confiscated in appropriate circumstances but will not be kept overnight unless specific reasons can be given. Parents will be informed quickly in these cases. Students may also be prevented from bringing a mobile electronic device into the School temporarily or permanently.

10.7 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

11 Photographs, images and moving images (photographic).

11.1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

11.2 Individuals may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image. This includes the posting of said material to any online platform.

11.3 Students must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.

11.4 The posting of images which in the reasonable opinion of the School is considered to be offensive or which brings the School into disrepute on any form of social media platform, or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

11.5 Please see the School's Online Safety Policy, (Annex 3 Taking or storing and using Images of Children), available on the School's website.

11.5 Sexting (Sexual Imagery)

11.5.1 'Sexting' means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet.

11.5.2 Sexting is strictly prohibited, whether or not the student is in the care of the School at the time the image is recorded and / or shared.

11.5.3 Sexting may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

11.5.4 Remember that once a photo or message is sent, individuals have no control about how it is passed on. The image may have been deleted, but it could have been saved or copied and may be shared by others.

11.5.5 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

11.5.6 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Child Protection and Safeguarding policy and procedures).

11.5.7 Any image received, sent or forwarded or otherwise seen, individuals should speak to any member of staff or line manager for advice.

12. Responsibilities

12.1 This policy is the responsibility of the Director of IT and Designated Safeguarding Lead.

12.2 The Bursar and Director of IT are responsible for ensuring that issues around data protection and copyright compliance are monitored.

12.3 All Staff are responsible for the implementation and monitoring of the policy.

12.4 The responsibility for the supervision of the Acceptable Use Policy is delegated to the Director of IT and the IT Support Team by the SLT. Any suspected breach of this policy should be reported to a member of IT Support staff or line manager. A responsible senior member will then take the appropriate action within the School's disciplinary framework; other members of the School's IT Support staff will also act when infringements are detected in the course of their normal duties. All incidents involving the safe use of technology will be logged.

12.5 The Designated Safeguarding Lead will consider the record of incidents and logs of internet activity as part of the ongoing monitoring of safeguarding procedures.

12.6 Consideration of the efficiency of the School's online safety procedures and the education of students about keeping safe online will be included in the Governors' annual review on safeguarding.

Appendix 1

1. IT Services Acceptable Use Policy (AUP) Summary for Students

1.1 **You must not:**

1.1.1 Allow other people to use your account or share passwords.

1.1.2 Download or access illegal software onto a workstation or personal device while using the School network.

1.1.3 Download or copy any software packages from the School network onto portable media, etc.

1.1.4 Upload your own personal software packages onto a School workstation.

1.1.5 Access offensive or abusive material.

1.1.6 Send offensive, abusive or inappropriate e-mails. If you receive an abusive or inappropriate email you should inform a member of staff.

1.1.7 Access "inappropriate" websites - some Internet pages are illegal and may be subject to criminal proceedings.

1.1.8 Interfere with another users' work.

1.1.9 Photograph or record members of staff or students without their permission, using devices such as mobile phones, cameras or digital recorders.

1.1.10 Use software designed to unblock sites, (such as VPN's).

1.1.11 Use online gambling sites.

1.1.12 Use peer-to-peer and related applications anywhere on school premises. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus and KaZaA.

1.1.13 Abuse equipment.

1.1.14 Make offensive or inappropriate comments including bringing the School's name and reputation into disrepute on any forum/platform, such as social media sites (whether using a school device or not) where a connection between the user and the School can reasonably be made.

1.2 Please remember, when in teaching and learning areas such as the Library, IT Suites or classrooms:

1.2.1 Keep noise to a minimum to avoid disrupting others.

1.2.2 Copyright regulations apply to electronic sources - please check before you print out from online services.

1.2.3 No unauthorised use of chat rooms.

1.2.4 Logout or lock your computer when leaving a computer, even for a short time.

1.2.5 Be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc) has been electrically tested, before using it on School premises.

1.3 Anyone found abusing the School policy on the use of computers may have their network rights removed and may be subject to further disciplinary action.

1.4 School computers are provided primarily for School work. However, you may use the equipment for personal use providing:

1.4.1 You do not breach the Acceptable Use Policy and Online Safety Policy.

1.4.2 You are not doing so for gambling purposes.

1.5 If you use the School equipment for personal use you should note the following:

1.5.1 Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.

1.5.2 If you are using communal IT facilities (such as the library), you may be asked to log-off where the demand for the equipment is high.

1.5.3 This Acceptable Use Policy applies to both wired and wireless access and use of network on your own equipment or on School equipment.

1.5.4 In order to use the IT Facilities of the School you must first be properly registered to use such services.

1.5.5 Registration to use School services implies and is conditional upon acceptance of this Acceptable Use Policy.

1.5.6 The lack of a signature does not exempt an individual from any obligation under this policy.

1.5.7 The continuing use of the IT Facilities will be deemed to be acceptance by the user of the terms of this policy.

1.6 The use of personal equipment is only allowed in School in the following circumstances

1.6.1 The personal use of equipment is not allowed in lessons unless in years 12 and 13 with expressed agreement from a teacher.

1.7 Students who are in the above list must only connect their personal device to the “LPS Wireless” network. Students are not permitted to connect their device directly via cable to any network socket within the organisation or to any other Wi-Fi network that the school transmits.

1.8 The school reserves the right to remove access to IT services at any time. Students must abide by all this policy when their device is connected to the school network. This is a summary of the IT Acceptable Usage Policy (Students). The full policy including further details can be found on the School website.

Author:	Eddie Falshaw, Deputy Head/David Pacey, Director of ICT
Sign off:	Matthew Judd, Head
Date of last review:	June 2019
Date of next review:	June 2021
Publication:	Z:\Policies\Current Policies\IT Acceptable Use Policy V:\School Policies\IT Acceptable Use Policy http://www.leightonpark.com/About/Policies