Network Acceptable Use Policy (Pupils)

Lancing College & Lancing College Preparatory Schools

Lancing College

1 Introduction

1.1 It is the responsibility of all users of Lancing College's I.T. services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

2 Purpose

2.1 This policy defines the acceptable use of the Lancing College network in order to protect the Lancing College Network and systems from risks including data loss, viruses and hacking. This acceptable use policy covers general secure practice for computing devices and should be read in conjunction with the other IT policies.

3 Acceptable Use Policies

3.1 The following acceptable use policies are attached as appendices to this document:

• Email Acceptable Use Policy	Appendix A	Page 6
• Internet Acceptable Use Policy	Appendix B	Page 11
• College Laptop Acceptable Use Policy (Pupils)	Appendix C	Page 16
• iPad/BYOD Acceptable Use Policy (Pupils)	Appendix D	Page 18

4 Accessing the Lancing College Network

Users are provided with an IT induction when they join the College. This gives users a basic understanding of the system and how it should be used. Once complete the user receives their logon details which includes a Username and Password.

4.1 Users must:

- keep their password secure and not disclose said password;
- ensure they do not allow anyone else to use their logon details;
- ensure their password is at least 8 characters in length, with at least one capital letter, one lower case letter and a number within the password;
- change their password every term if they are a member of staff or yearly if they are a pupil. This change will be enforced by the IT Department.

5 Ensuring Data Confidentiality (See Data Protection Policy for further details)

5.1 Ensure a computer is locked or logged off whenever it is left unattended.
5.2 Take care when working in a space with others present, for example; protect password input, if sensitive information is on screen consider the working location and if it is suitable for the audience.

6 Unacceptable Use

6.1 The College network may not be used directly or indirectly by a user for the access, download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- unsolicited “nuisance” emails;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the College or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings the College into disrepute.
- websites or material that is deemed illegal or inappropriate. These include (but not exclusively) – Pornographic websites, websites promoting illegal activities for example hacking or illegal gambling, terrorist related websites and websites promoting illegal drugs

6.2 The College network must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

- intentionally wasting staff effort or other College resources;
- corrupting, altering or destroying another user’s data without their consent;
- disrupting the work of other users or the correct functioning of the College network; or
- denying access to the College network and its services to other users.

6.3 Where the College network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College network.

6.4 Users shall not:

- introduce data-interception, password-detecting or similar software or devices to the College’s Network;
- seek to gain unauthorised access to restricted areas of the College’s Network;
- access or try to access data where the user knows or ought to know that they should have no access;
- carry out any hacking activities; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

7 General Use and Privacy

7.1 For security and maintenance purposes the IT department may monitor all data, systems and network traffic at any time to ensure compliance with this and other policies and the effective operation of the College’s systems.

7.2 The theft or loss of any Lancing College or personally owned IT equipment that is held on site should be reported to the IT Department as well as the Lancing College Security Manager.

7.3 Lancing College recognises that removable media devices (such as USB memory sticks, portable hard drives) can greatly benefit users who are often mobile. However such devices are a well-known source of malware infections, and can result in the loss of sensitive information. As such, users should not store any sensitive information on such devices.

8 Backup Procedure

8.1 All sensitive, valuable or critical information that resides on the file servers at Lancing College are backup up on a nightly basis. The backups are replicated from one end of the campus to the other to protect against major damage occurring at the primary location and are also replicated to the cloud.

8.2 In order to prevent the loss of any data, users are responsible for:

- Ensuring their work is saved to the network so that it will be backed up.

9 Protection from Viruses

9.1 All computers connected to the Lancing College Network must operate up-to-date antivirus software.

9.2 Files shared, downloaded or received by email may contain viruses. If in any doubt it should be reported to the IT Department.

10 Remote Access Procedure

10.1 Users with remote access privileges are responsible for ensuring that their remote access connection is given the same consideration as the users on-site connection to the College network.

10.2 Remote connections to the College network are subject to the same rules and regulations, policies and practices outlined in this policy and its supporting policies.

10.3 Remote access users must not divulge their login details to anyone else.

10.4 Remote access users must not save their password within their internet browser as this can create an automatic connection when authentication is no longer needed.

11 Consequences of Breach

11.1 In the event of a breach of this Acceptable Use Policy by a User the College may in its sole discretion:

- restrict or terminate a user’s right to use the College network;
- the College may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its internal policies;
- inform the appropriate authorities if actions or conduct is deemed unlawful.

12 References

12.1 Data Protection Policy

Author:	Andy Brown, Director of IT	June 2017
Annually Reviewed:	Andy Brown, Director of IT	May 2025
Next Scheduled Review:		May 2026

Appendix A

EMAIL ACCEPTABLE USE POLICY

1. Introduction

1.1. Staff and Pupils need to be aware that e-mail carries exactly the same status as other forms of communication, including letters, memos and telephone conversations, and the same consideration and legal implications need to be applied and observed in the use of e-mail as in these other forms of communication.

2. Scope of the Policy

2.1. This policy applies to all staff and pupils who use the College's IT facilities and sets down the standards which staff and pupils are required to observe in the use of e-mails. It covers:

i. Electronic Mail services within Lancing College Local Area Network (internal e-mail).
ii. Electronic Mail sent through the Internet to other organisations/individuals (external e-mail).
iii. The safeguarding of information sent by e-mail.

It is the responsibility of all pupils to acquaint themselves and comply with this policy.

3. General

3.1. The College provides an e-mail system to support its academic and business activities and access to e-mail facilities for all staff and pupils is granted on this basis. In addition at specified times and locations staff and pupils may access the facilities for personal activities including communication and recreational use. Staff and Pupils are reminded that e-mail sent and received on the College's systems are not private property they remain part of the College's information systems. Personal use should never compromise availability for academic or business use.

3.2. When composing and sending an e-mail, it is expected that the content meets the standards of professionalism which Lancing College expects of its staff and pupils.

3.3. Staff and Pupils should only write that which they would speak in an open forum and should be aware that UK legislation, including the laws of libel, applies to electronic documents as well as manuscript. Therefore, staff and pupils should think carefully about what is said about other individuals or organisations when composing and sending e-mail messages.

3.4. It is not permitted for staff or pupils to send sexual, racially biased or other inappropriate e-mails, which would infringe the School's code of conduct.

3.5. Do not use aggressive, abusive or deliberately anti-social language. Never e-mail hastily or out of anger.

3.6. Use of personal e-mail must not detrimentally affect the duties of other staff or pupils or disrupt the system, and/or harm the College's image or reputation.

3.7. Staff and Pupils should be aware that a disclaimer is automatically added to all external E-mails when it leaves our system. The following wording will be automatically added to E-mail:

****CONFIDENTIALITY NOTICE AND LEGAL LIABILITY WAIVER****

The content of this email and any attachments are CONFIDENTIAL and may contain privileged information. If you are not the addressee it may be UNLAWFUL for you to read, copy, distribute, disclose or otherwise use the information contained herein.

The content of this message and/or attachments may not reflect the views and opinions of the originating company or any party it is representing.

Lancing College Limited. Registered in Cardiff Number 3779985. A Registered Charity Number 1076483

Buxbrass Limited. Registered in Cardiff Number 1570797.

Registered Office for all companies:

Lancing College
Lancing
West Sussex
BN15 0RW

4. External and Internal E-mail

4.1. All staff and pupils must be aware that their external e-mail address is an Academic Business address. The College retains ownership of any information transmitted and that such messages will be taken as representing Lancing College. The same standards of business courtesy must be applied as in the case of any other form of communication undertaken on behalf of the College.

4.2. Staff and Pupils should not copy or download or forward material that is obviously libellous (or otherwise unlawful), unrelated to work, or inappropriate in any way, i.e. graphic images, sound files, or music.

4.3. Staff and Pupils are responsible for keeping their e-mail address books up to date and are reminded of Principle 4 of the Data Protection Act 1988 which states that personal data shall be accurate and, where necessary, kept up to date.

4.4. Staff and Pupils are reminded that they are responsible for their own e-mail housekeeping. Unwanted and non relevant e-mail should be deleted regularly, and archiving routines should be set up on e-mail which needs to be retained. If staff or pupils are unsure how to achieve this, guidelines are available from the IT department.

4.5. Staff and Pupils must ensure that they have the appropriate authority to e-mail on a particular issue.

4.6. Staff and Pupils should not give their external e-mail address out carelessly. Only enter it on business circulars and application forms if you are sure that it will not be misused or forwarded on. E-mail circulation lists operate in the same way as junk mail; continuity of service can be seriously affected by unsolicited messages, some of which may contain malicious code or virus.

4.7. Staff and Pupils should, where possible, avoid sending large graphics or scanned images.

5. Confidentiality

5.1. Particular attention should be paid to the addressee to ensure the message will reach the intended recipient especially if choosing from an address list of similar names or using the auto fill within Outlook.

5.2. Messages intended for another recipient should be re-directed and then deleted. Any incorrectly addressed messages should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

6. Security

6.1. Lancing College has in place a firewall to ensure the safety and security of the School's networks. Additional devices may also be installed in the future to further protect these networks. Any member of staff or pupil who attempts to disable, defeat or circumvent any of the College's security facility will be subject to disciplinary action.

6.2. Staff and Pupils must not allow other users to use their network login; it would allow unsolicited e-mail to be sent on your behalf, and give access to College applications using your login details. Do not leave your PC unattended whilst logged in, please ensure it is locked or logged off. As a standard the college uses a password protected screen saver which activates after 10 minutes of inactivity.

6.3. Lancing College use Exchange Online Protection which is an email filtering service. All incoming and outgoing messages are scanned by the filter to check for any viruses, spam email etc. Whilst this is never going to be 100% effective it picks up a very large majority of unwanted emails.

6.4. Anyone who believes that they have received a message that includes malicious code (virus), must not open it but report it to the IT department immediately.

6.5. It is extremely common for a virus to propagate itself via an e-mail attachment. Commonly the attachment will be an executable file (with .exe, .vbs suffix) or a link to an external site. If there is any doubt as to the authenticity of an e-mail attachment, it must not be opened; report it to the IT department immediately.

6.6. It is also common for a virus to use the Outlook address book to forward itself to others; this is how many viruses spread so quickly. This means that infected e-mail could be received from a known and trusted source. Staff and Pupils should be immediately suspicious if the email is unusual in any way.

6.7. There are many different types of unwanted email including spam emails and phishing emails. It is important to ensure these emails are not replied to and any links in the emails are not clicked as this could launch malicious code or take you to hoax site where you will be asked for personal details.

7. Monitoring and Misuse

7.1. Lancing College has systems in place that monitor and record all e-mail usage. E-mail must be used for College and not normally for personal purposes (during College hours), no member of staff or pupil should have any expectation of privacy as to his or her e-mail use. Incidental and occasional use of e-mail for personal reasons is permitted subject to the restrictions contained within this policy. Any personal use is expected to be in the person's own time and must not interfere with his or her responsibilities. Use of personal e-mail must not detrimentally affect others, disrupt the system, and/or harm the College's image or reputation.

7.2. Lancing College maintains the right and ability at any time and without prior notice, where justified:

- To inspect any information stored on College computing facilities in order to ensure compliance with the policy; and
- To remove the e-mail facility from any pupil who fails to observe the Policy.
- This helps ensure compliance with internal policies and the law. In order to ensure compliance with this policy, the College reserves the right to employ monitoring software to check on the use and content of e-mail to ensure that there are not breaches of the policy.
- Abuse or misuse of the e-mail system will be subject to disciplinary action in accordance with Lancing College's disciplinary policy.

7.3. Examples of e-mail misconduct are where the content of which might be considered:

- Indecent, obscene, pornographic or illegal
- Offensive, abusive, in that its context is or could be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful to encourage or promote activities which make unproductive use of College time
- Involve activities outside the scope of your responsibilities; for example, unauthorised selling/advertising of goods or services.
- To affect or have the potential to affect the performance of, damage or overload the College's systems, network and/or external communications in any way
- Would be in breach of copyright or licence provision with respect to both programmes and data

If clarification of any aspects of policy are required, refer to the IT department.

8. Further Information

8.1. As part of our data protection policy it is essential that the following guidance is used when sending emails, particularly those that are being sent externally:

- BCC – Always use the BCC field when sending email to multiple contacts externally. This ensures none of the intended recipients can see each other's email addresses.

- Autocomplete – Be careful when using the autocomplete email address function when composing emails, it is easy to select the wrong recipient when so many people have similar names.

- Distribution Lists – When sending to groups of people via a distribution list make sure you are aware who is a member of that list before you send the email.

- Forwarding – When forwarding emails always check the existing content (conversations and email addresses) to ensure there is nothing in there that should not be sent to the intended recipient.

- Sensitive Data – If there is a need to send sensitive data through the email system it should be in the form of a link to a secure location, for example a section of the VLE accessible to the relevant people only, rather than in the email body itself or in an attachment.

Author:	Andy Brown, Director of IT	June 2017
Annually Reviewed:	Andy Brown, Director of IT	May 2025
Next Scheduled Review:		May 2026

Appendix B

INTERNET ACCEPTABLE USE POLICY

1. Purpose

1.1. This policy applies to all Staff and Pupils (Network Users) who use the College's Internet facilities and sets down the standards which the users are required to observe in the use of the internet.

1.2. It is the responsibility of all network users to acquaint themselves and comply with this policy. Certain terms in this policy should be understood expansively to include related concepts:

- School/College includes all Lancing College locations and both academic and non-academic areas.
- Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so called HTML files read in an internet browser, any file meant to be accessed by a word processing or desk-top publishing programme or its viewer or any other electronic publishing tools.
- Graphics includes photographs, pictures, animations, movies or drawings.
- Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions, smartboards, CleverTouch boards and virtual-reality tools.

2. General

2.1. Use of the Internet by all network users is permitted and encouraged where such use is suitable for school purposes and supports Lancing College's aims. In addition, network users may access the facilities outside of core college hours for personal activities including communication and recreational use. Personal use should never compromise availability for academic or business use.

2.2. The College day is defined as follows:

Lesson/Academic Times: Monday - Friday 08:20 – 18:00, 19:00 – 21:00
Saturday 08:20 – 12:30

Non – Lesson Times:
Lunch Monday – Friday 13:05 – 14:20
Before Evening School Monday – Friday 18:00 – 19:00
After Evening School Monday – Friday 21:00 – 23:00
Weekends Saturday 12:30 – 23:00
Sunday 08:20 – 23:00

2.3. The Internet is not available to any Pupil after 23:00 each night with the exception of the Sixth Form who have access until midnight on Saturday evenings only. Staff are not time limited.

2.4. Use of the Internet is to assist the College's objectives and therefore the College provides access to the vast information resources of the Internet to help access relevant material. The facilities to provide that access represent a considerable commitment of this College's resources for communications, networking and software. This Internet usage policy is therefore designed to help you understand the College's expectations for the use of those resources in the particular conditions of the Internet and to help you use those resources properly.

2.5. The types of attack that the College will be exposed to via the Internet are many; for example, intrusion and information theft, denial of service (to stop us from using our systems), and corruption of the College's data (through hackers and viruses).

2.6. In addition, some areas of the Internet contain illegal material which if accessed could lead to criminal proceedings against you and the College. Such a position is clearly untenable and this policy exists to protect Lancing College and its staff and pupils.

3. Use of the Internet

3.1. By logging on to the College's network you signify your acceptance of this policy and other published IT policies, and you should seek clarification of any issues that you do not understand.

3.2. The policy is one of a range of College policies of which you should be aware, including Lancing College Network Acceptable Use, E-mail Acceptable Use, iPad/BYOD Acceptable Use, and the Mobile Phone and Devices Acceptable Use policy. It is your responsibility to make sure that you abide by the College's policies. Failure to do so may result in disciplinary action.

3.3. The Internet is to be used in a manner which is consistent with Lancing College's standards of professional business conduct and as part of academic research.

3.4. During College hours we expect Internet access to be for College related purposes only to research relevant topics and obtain useful College related information.

3.5. We insist that you conduct yourself honestly and appropriately on the internet and respect the copyrights, software licensing rules, property rights, data protection guidelines, privacy and prerogatives of others, just as you would in any other circumstances.

3.6. All existing College policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of College resources, sexual harassment, fraud and information security.

3.7. You must not use the Internet for unnecessary or unauthorized work. This type of Internet usage causes congestion and slows other network users, takes away from work or study time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also result in negative publicity for Lancing College and expose the College to significant legal liabilities, such usage will therefore result in disciplinary action.

3.8. The chat-rooms, newsgroups, mailing lists and e-mail of the Internet give each individual Internet user an immense and unprecedented reach to propagate corporate College messages. Because of that power you must take special care to maintain the clarity, consistency and integrity of the College's professional image and posture.

3.9. Anything any one network user writes in the course of acting for the College on the Internet can be taken as representing the College's official posture. This is why we expect you to forgo a measure of your individual freedom when you participate in chat-rooms, mailing lists or newsgroups on College business, as outlined below.

3.10. The College retains the copyright to any original material posted to any forum, newsgroup, chat-room or web page by any pupil in the course of his or her studies.

3.11. Where possible, network users should schedule resources-intensive operations such as large file transfers, video downloads, mass e-mailing and the like for off-peak times.

3.12. Any file, including e-mails, that is uploaded or downloaded must be scanned for viruses before it is run or accessed. This is done automatically on the College network but users must check that their anti-virus software is running and up to date if working from a personal device. Ask for advice from the IT department if you are unsure how to do this.

3.13. Video and audio streaming and downloading technologies represent significant data traffic, which can cause local network congestion. Video and audio downloading should be avoided where possible.

3.14. Network Users should be especially careful not to disclose any personal or identifying details when using newsgroups or chat-rooms. Avoid the use of names, telephone numbers and locations. Under no circumstances should personal or College addresses be given out.

4. Inappropriate Use of the Internet

4.1. The display of any kind of indecent image or document, for example sexually explicit or offensive material, on any School system is a violation of Lancing College policies on security and harassment. In addition, indecent material may not be archived, stored, distributed, edited or recorded using the College's network or computing resources.

4.2. The College's Internet facilities and computing resources must not be used knowingly to break the law. Use of any College resources for illegal activity is grounds for immediate discipline and the College will co-operate with any legitimate law enforcement agency.

4.3. Any legal and licensed software or files downloaded via the Internet into the College network become the property of Lancing College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

4.4. No network user may use College facilities knowingly to download or distribute pirated (illegal and unlicensed) software or data.

4.5. No network user may use the College's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of another network user. VPN use is strictly prohibited.

4.6. No network user may use the College's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of another network user. VPN use is strictly prohibited.

4.7. Use of College internet access facilities to commit acts such as misuse of College assets or resources, sexual harassment, unauthorised public speaking and misappropriation or theft or intellectual property are specifically prohibited and any such action(s) will result in disciplinary action being pursued against the individual.

4.8. Network users are specifically prohibited from downloading any software without the express permission of the IT department.

4.9. Network users with Internet access may not use College Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.

4.10. Network users with Internet access may not use College Internet facilities to download images or videos unless there is a College related use for the material.

4.11. Network users with Internet access may not upload or copy any software licensed to the College or data owned or licensed by the College without explicit authorisation from the member of staff responsible for the software or data.

5. Monitoring Internet Use

5.1. Internet access is available to all network users with access to a computer/laptop/tablet which is connected to the College's networks. The College has systems in place that can monitor and record all Internet usage. The College wants network users to be aware that its security systems record (for each and every person) each web site visit, each chat-room, newsgroup or e-mail message and each file transfer into an out of its internal networks. No network user should have any expectation of privacy as to his or her Internet usage. The IT department will review internet activity and analyse usage patterns, and may choose to publicise this information to ensure that College internet resources are devoted to maintaining the highest levels of productivity.

5.2. Lancing College reserves the right to inspect any and all files stored on College computing facilities in order to assure compliance with this policy.

5.3. The College uses independently supplied software (called Fortigate) to identify, block and report access to all such inappropriate Internet sites. The College may block access from within its networks to all such sites that it knows of. If you find yourself connected accidentally to a site that contains illegal, sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating programme. More likely you may find you have been blocked from accessing such sites and will receive the 'Fortigate' denial page indicating this.

5.4. You must report each incident (even accidental) of this type to the IT department for investigation.

5.5. Fortigate provides access to web pages on the Internet by use of a categorization system. Every web page is categorized according to its content, and facilities exist to block access to certain categories; for example access is blocked to sites categorized as pornography, sport, criminal content etc.

5.6. It is acknowledged that certain network users may require, during the normal course of, their work or studies access to certain sites that may normally be blocked. It is possible to make exceptions in these cases to allow legitimate access, by contacting the IT department; please note that a senior member of staff may be required to confirm the requirements before access is granted.

5.7. Internet access is extended after (and before) working hours, in that the category restrictions are relaxed. For example access to Social Media, Mail etc is allowed.

6. Confidentiality

6.1. Network users are reminded that chat-rooms, mailing lists and newsgroups are public forums where it is inappropriate to reveal confidential College information and any other material, covered by data protection and College policies/procedures.

7. Security

7.1. While our direct connection to the Internet offers potential benefits, it can also open the door to some significant risks to our information and systems if we do not follow appropriate security disciplines. The overriding principle is that security is to be of paramount concern and network users must follow the agreed procedures.

7.2. A NETWORK USER WILL BE HELD ACCOUNTABLE FOR ANY BREACHES OF SECURITY OR CONFIDENTIALITY.

7.3. The College has in place a firewall to ensure the safety and security of the College's networks. Additional devices may also be installed in the future to further protect these networks. Any network user who attempts to disable, defeat or circumvent any College security facility will be subject to immediate disciplinary proceedings.

7.4. Any files containing sensitive or confidential College information that are transferred in any way across the Internet must be encrypted. Advice and assistance may be sought from the IT department.

7.5. Connections to the Internet using VPNs / wireless dongles / phone tethering is specifically prohibited.

7.6. Usernames and passwords help maintain individual accountability for Internet resource usage. Any network user who obtains a password or username for an Internet resource must keep that password confidential.

Author:	Andy Brown, Director of IT	June 2017
Annually Reviewed:	Andy Brown, Director of IT	May 2025
Next Scheduled Review:		May 2026

Appendix C

COLLEGE LAPTOPS ACCEPTABLE USE POLICY (PUPILS)

1.

1.1. ‘Laptop’ refers to the ‘College-provided laptop’ throughout**.**

1.2. Lancing College has recognised that laptops are a very useful additional educational tool in the development of students’ Computer Science skills.

1.3. Students undertaking the Computer Science course will be provided with a College laptop by the school’s IT Department. Use of the laptops is subject to the College’s general rules as well as the specific codes of conduct for ICT and the Internet, in addition to these laptop specific guidelines.

1.4. Students will be required to sign for receipt of their laptops and in so doing they will agree to abide by all regulations governing their use. Students’ use of their laptop will be reviewed periodically.

1.5. Laptops are College property and are loaned to students for a fixed period, normally of two or three years; they must be returned to the College on request and if the student leaves before the end of this period. Students may be asked to show their laptop’s content and applications to any member of the College staff at any time. In cases of inappropriate use, the student may face appropriate disciplinary sanctions and the laptop may have to be returned to the College.

1.6. Laptops are the responsibility of the students who must keep their laptop & charger in a case when in transit and left in a secure locked location when not in use. Students should maintain appropriate security when taking the laptops off the College premises as they are not insured by the College for loss or theft. Parents may wish to make their own arrangements.

1.7. Any damages to laptops must be reported to the IT Department immediately. The IT department will arrange for the damage to be repaired. Under no circumstances should a pupil do this themselves. Damage claims will be added to the pupils’ end of term bill.

2. General

2.1. Students are required to bring their laptop and charger in the case provided to Computer Science lessons. The device must be charged daily and there should always be sufficient storage space to allow the student’s academic work to be carried out as directed.

2.2. The charger must not be left plugged in when the laptop is unattended or overnight while the student is sleeping. Adequate ventilation must be available for both laptop and charger to ensure that neither become unnecessarily hot.

2.3. Students must maintain personalised password protection on their laptop and take reasonable care to avoid degradation of the laptop. Careless or deliberate damage to laptops will be chargeable.

2.4. Laptops are only to be used in class for academic activities with the teacher’s permission.

2.5. When not in use laptops should be closed in their cases.

2.6. Images, still or video, or recordings of any nature must not be made without the subject's express permission.

2.7. Material attributable to Lancing College, through any media, may not be published outside the College environment without specific permission from the College.

2.8. During teaching periods communication via text / email / chat or any other media is not permitted without specific permission from a teacher.

2.9. Use the laptop for personal entertainment or data storage, providing sufficient space is left for academic purposes.

2.10. Support with laptop-related matters is available in the usual way from IT Support.

2.11. Problems with, or damage to laptops must be reported immediately to IT Support.

2.12. A lost laptop must be reported to IT Support immediately.

3. Appropriate Use

3.1. Students must not:

- Modify the laptop in any way other than instructed by the administrator or other College personnel.
- Exchange laptops with another student or allow their laptop to be used by another student.
- Apply any permanent marks, decorations, or modifications to the laptop, charger or case.

3.2. Students may:

- Use the laptop for personal entertainment or data storage, providing sufficient space is left for academic purposes. Any personal data stored on the laptop should also be backed up to a personal device or cloud storage as the device may need to be returned or rebuilt at any point so the College will not take responsibility for any lost data held on the laptop.

3.3. **Support**:

- Support with laptop-related matters is available in the usual way from IT Support.
- Problems with, or damage to laptops must be reported immediately to IT Support.
- A lost laptop must be reported to IT Support immediately.

Author:	Andy Brown, Director of IT	June 2017
Annually Reviewed:	Andy Brown, Director of IT	May 2025
Next Scheduled Review:		May 2026

Appendix D

iPAD/BYOD ACCEPTABLE USE POLICY (PUPILS)

1.

1.1. ‘iPad’ refers to the ‘College-provided iPad’ throughout. ‘BYOD’ refers to a pupil’s own device throughout.

1.2. Lancing College has recognised BYOD and iPads are a very useful additional educational tool in the armoury of the modern pupil. They will afford many opportunities for independent and collaborative learning, in addition to certain organisational benefits.

1.3. Students will bring their own device to school from September 2022 or will have been provided with a College iPad that will be centrally managed by the school’s IT Department if they started before that. Use of BYOD/iPads is subject to the College’s general rules as well as the specific codes of conduct for ICT and the internet, in addition to these BYOD/iPad specific guidelines. It should be remembered that these iPads are owned by the college and pupils own devices are owned by the student.

1.4. Students will be required to sign for receipt of their iPads and in so doing they will agree to abide by all regulations governing their use. Students’ use of their iPad will be reviewed periodically. Students bringing their own devices and connecting them to the College wifi network are also agreeing to abide by all regulations governing their use.

1.5. iPads are College property and are loaned to students for a fixed period, normally of two or three years; they must be returned to the College on request and if the student leaves before the end of this period. Once the loan period is up pupils can buy the device at a discounted rate or return the iPad, charging block and cable. Students may be asked to show their iPad’s content and applications to any member of the College staff at any time. In cases of inappropriate use, the student may face appropriate disciplinary sanctions and the iPad may have to be returned to the College.

1.6. iPads are insured from the first accidental damage whilst in College up to the sum of £100 but are the responsibility of the students who must keep their iPad in the case at all times and left in a secure locked location when not in use. Students should maintain appropriate security when taking the iPads off the College premises as they are not then insured by the College for loss or theft. Parents may wish to make their own arrangements.

1.7. Any damages to iPads must be reported to the IT Department immediately. The IT department will arrange for the damage to be repaired. Under no circumstances should a pupil do this themselves. The College will cover the cost of the first accidental damage claim, up to the sum of £100, but subsequent claims will be added to the pupils' end of term bill.

1.8. Students’ own devices are their property and they should have adequate insurance to cover damages. The College reserves the right to confiscate a student’s device if deemed necessary and investigate it's contents if it forms part of a disciplinary or safeguarding investigation.

2. General

2.1. Students are required to bring their BYOD/iPad to all lessons. The device must be fully charged daily and there should always be sufficient storage space to allow the student's academic work to be carried out as directed.

2.2. Students must maintain a lock code or password protection on their iPad. The lock screen image must clearly identify the pupil by their name and House. Students must adhere to iPad security storage as directed when iPads are not in use. Careless or deliberate damage to iPads will be chargeable. We strongly recommend student have a lock code or password on their own devices as well.

3. In the Classroom

3.1. BYOD/iPads are only to be used in class for academic activities and with the teacher's permission.

3.2. When not in use BYOD/iPads should be turned off.

4. Appropriate Use

4.1. Images, still or video, or recordings of any nature must not be made without the subject's express permission.

4.2. Material attributable to Lancing College, through any media, may not be published outside the College environment without specific permission from the College.

4.3. During teaching periods communication via text / email / chat or any other media is not permitted without specific permission from a teacher.

5. Students should not:

5.1. Modify the iPad in any way other than instructed by the administrator or other College personnel.

5.2. Remove the iPad case unless specifically asked to do so by the IT department.

5.3. Exchange iPads with another student or allow their iPad to be used by another student.

5.4. Use another student's iPad.

5.5. Apply any permanent marks, decorations, or modifications to the iPad or case.

5.6. Clear or disable browsing history on the iPad.

5.7. Change the college Apple ID to a personal Apple ID.

5.8. Use two form authentication on the college Apple ID.

6. Students may:

6.1. Use the BYOD/iPad for personal entertainment or data storage, providing sufficient space is left for academic purposes.

7. Support

7.1. Support with BYOD/iPad-related matters is available in the usual way from IT Support.

7.2. Problems with, damage to or loss of iPads must be reported immediately to IT Support. For BYOD pupils can ask IT Support for assistance with getting the device repaired.

Author:	Andy Brown, Director of IT	June 2017
Annually Reviewed:	Andy Brown, Director of IT	May 2025
Next Scheduled Review:		May 2026