



LISAL

LANCASTER INDEPENDENT SCHOOL
FOR ALTERNATIVE LEARNING

Acceptable Use Policy (ICT)

Version date: January 2026

Document review period: September – November 2027



Contents

1. Introduction and aims	3
2. Relevant legislation and guidance	3
3. Definitions	4
4. Unacceptable use	4
5. Staff (including trustees, volunteers, and contractors)	5
6. Students	8
7. Parents	9
8. Data security	9
9. Internet access	11
10. Monitoring and review	11
Appendix 1: Acceptable use of the internet: agreement for parents and carers	12
Appendix 2: Acceptable use agreement for Class 5 students only	13
Appendix 3: Acceptable use agreement for students in lower schools, except Class 5	14
Appendix 4: Acceptable use agreement for staff, Trustees, volunteers and visitors	15
Appendix 5: Bring Your Own Device (BYOD) Agreement for Staff	16
Appendix 5: Bring Your Own Device Agreement for staff, Trustees and volunteers	16



Acceptable Use Policy

1. Introduction and Aims

Information and Communication Technology (ICT) is a vital part of our school's operations and supports teaching, learning, pastoral care, and administration. However, its use also presents risks related to data protection, online safety, and safeguarding.

This policy aims to:

- Set clear guidelines for the appropriate use of the school's ICT facilities
- Establish expectations for online conduct across the school community
- Support the school's policies on data protection, safeguarding, and online safety
- Prevent misuse or disruption of ICT systems
- Promote safe and responsible ICT use among students

Scope: This policy applies to all users of the school's ICT facilities, including trustees, staff, volunteers, contractors, parents, visitors, and students. Breaches may lead to disciplinary action in line with the Employee Handbook.

Associated Policies:

- Online Safety Policy
- Safeguarding Policy
- Whole School Behaviour Policy
- Data Protection Policy
- Use of Image Policy
- Social Media and Electronic Devices (Employee Handbook)

2. Relevant Legislation and Guidance

This policy is in line with the following legislation and guidance:



- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990
- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- *Keeping Children Safe in Education (2023)*
- *Searching, Screening and Confiscation – Advice for Schools (2018)*

3. Definitions

- **ICT Facilities:** All hardware, software, systems, and services provided by the school, including devices, network infrastructure, websites, and future technologies.
- **Users:** Anyone authorised to use school ICT facilities (staff, trustees, students, volunteers, contractors, visitors).
- **Personal Use:** Any non-work-related use of ICT facilities.
- **Authorised Personnel:** Staff designated to manage, administer, or monitor ICT systems.
- **Materials:** Any data or files created using ICT facilities, including documents, photos, videos, audio files, websites, and social media content.

4. Unacceptable Use

Use of the school's ICT systems must not:

- Infringe copyright or intellectual property rights
- Bully, harass, or promote unlawful discrimination



- Breach school policies or procedures
- Involve illegal activities or promote illegal behaviour
- Share or create offensive, pornographic, or inappropriate material
- Defame or bring the school into disrepute
- Share confidential information without authorisation
- Connect unauthorised devices to the school network
- Install software, apps, or web services without approval
- Attempt to access restricted or password-protected information without permission
- Enable unauthorised access by others
- Intentionally damage equipment or systems
- Cause a data breach by sharing or accessing data without authorisation
- Use inappropriate or offensive language
- Promote private business interests (unless school-related)
- Attempt to bypass internet filtering mechanisms

This list is not exhaustive. The DSL will determine whether specific behaviour constitutes a breach.

4.1 Exceptions

Exemptions to the above may be granted at the discretion of the DSL. Requests must be submitted in advance via email.

4.2 Sanctions

Breaches of this policy may result in disciplinary action, in line with the Whole School Behaviour Policy or the Staff Disciplinary Procedures (Employee Handbook).

5. Staff (Including Trustees, Volunteers, and Contractors)

5.1 Access to ICT Facilities



Access to ICT systems and materials is managed by the Office Assistant. Staff are provided with individual login credentials. Any access issues or permissions concerns should be directed to the Office Assistant.

5.1.1 Phones and Email

- Staff must use their school email accounts for all work-related communication.
- Email content must be professional and appropriate, avoiding statements that could result in claims of defamation, harassment, or breach of confidentiality.
- All emails may be subject to disclosure under the Data Protection Act and must be treated as retrievable, even after deletion.
- Sensitive attachments must be encrypted.
- Accidental receipt or transmission of confidential emails must be reported to the DSL immediately.

School phones must not be used for personal matters. Mobile phones provided by the school must follow this Acceptable Use Policy.

5.2 Personal Use

Staff may use ICT facilities for limited personal use if:

- It does not occur during teaching hours or in the presence of students
- It does not interfere with job duties or others' use of facilities
- It does not involve storing personal media (e.g., music, photos)
- It does not constitute any 'unacceptable use' (see section 4)

Staff are reminded that all use of school ICT is subject to monitoring. Breaches may result in disciplinary action.

Bring Your Own Device (BYOD): Staff may use personal devices in line with the BYOD Agreement (Appendix 5). Personal ICT use, even outside school, can affect professional standing and must align with this policy.

5.2.1 Social Media

Staff must use personal social media accounts responsibly and with regard to their professional role. Guidance on Facebook security settings is provided in Appendix 1.

5.4 School Social Media Accounts



Only authorised personnel may manage or post on official school accounts (e.g. Facebook, Instagram). Posts are subject to professional judgement and must reflect the school's ethos.

5.5 Monitoring

ICT usage may be monitored, including but not limited to:

- Websites visited
- Bandwidth usage
- Emails
- Call records
- Access logs

Monitoring is conducted by authorised ICT staff, for purposes such as:

- Ensuring compliance with policies
- Investigating incidents
- Managing performance and operations
- Preventing crime
- Fulfilling legal obligations

6. Students

6.1 ICT Access

Students access ICT only under supervision during online safety sessions or curriculum-specific activities. Class 5 and some students with SEND may use devices with staff oversight.

Students are not permitted to bring mobile phones unless agreed with the school (see Safeguarding Policy).

6.2 Search and Deletion

Under the *Education Act 2011* and DfE guidance, the school may:

- Search student devices for prohibited content



- Delete data if it may disrupt learning or breach policy

6.3 Online Conduct Outside School

Students may face sanctions for unacceptable online activity outside school, including:

- Cyberbullying or harassment
- Sharing offensive, obscene, or pornographic material
- Breaching school policies
- Damaging the school's reputation
- Sharing confidential information
- Intentional damage to systems or data
- Data breaches
- Using offensive language

7. Parents

7.1 ICT Access

Parents do not have general access to ICT facilities. Those working with the school (e.g. volunteers or trustees) may be granted appropriate access and must adhere to this policy.

7.2 Online Communication

We encourage respectful communication online. Parents are expected to model appropriate behaviour when engaging with the school via social media or the website.

Parents are asked to sign the ICT and Online Communication Agreement in Appendix 2.

8. Data Security

The school takes reasonable measures to protect ICT systems and data, but users must also follow safe computing practices.

8.1 Passwords



- All users must set strong passwords and keep them secure.
- Passwords are managed by the network administrator.
- Suspected breaches must be reported to the School Manager immediately.
- Passwords should not be shared or written down unless securely stored.

8.2 Updates and Antivirus

All devices must be regularly updated and protected by antivirus software. Users must not bypass security features or safeguards.

8.3 Data Protection

All personal data must be handled in accordance with data protection laws and the school's Data Protection Policy (available in the School Policies folder).

8.4 Access Management

Access rights are managed by the Office Assistant. Users must not access data or systems beyond their authorisation. Unauthorised access must be reported immediately.

Devices must be locked when not in use and shut down at the end of the day.

8.5 Encryption and Personal Devices

Only authorised staff may use personal devices for school work or to access school data. These devices must meet security and encryption standards set by the Senior Leadership Team.

Refer to the Use of Image Policy and BYOD Agreement for additional guidance.

9. Internet Access

The school's internet connection is secured and filtered. Filters are reviewed every term.

Wifi access is not granted by default. It may be provided to parents volunteering in an official role or visitors requiring access for presentations or lessons

Staff must not share wifi credentials without authorisation.

10. Monitoring and Review



This policy is monitored by the DSL to ensure it remains current and effective. It is reviewed every two years and approved by the Board of Trustees.



Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
<p>Name of parent/carer:</p>	
<p>Name of child:</p>	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels:</p> <ul style="list-style-type: none"> ● Our official Facebook page ● Email/text groups for parents (for school announcements and information) 	
<p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none"> ● Be respectful towards members of staff, and the school, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure <p>I will:</p> <ul style="list-style-type: none"> ● Contact school directly to convey a grievance regarding member/s of staff so the school can address the issue appropriately and I will avoid using private groups, the school's Facebook page, or personal social media for this purpose. ● Contact an appropriate member of staff directly to convey a behaviour issue or incident involving student/s so the school can address the issue appropriately and I will avoid using private groups, the school's Facebook page, or personal social media for this purpose. ● Upload or share photos or videos on social media of my child ONLY, unless I have the permission of other children's parents/carers ● Not use my mobile phone inside the school building and/or in the school garden - except for taking photos of my child/children during public school events, such as school play or social gatherings. These photos will be SOLELY for personal use. 	
<p>Signed:</p>	<p>Date:</p>



Appendix 2: Acceptable use agreement for Class 5 students only

Acceptable use of the school's ICT facilities and internet: agreement for students (Class 5) and parents/carers

Name of student:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:



Appendix 3: Acceptable use agreement for students in lower schools, except Class 5

Acceptable use of the school’s ICT facilities and internet: agreement for students (lower school) and parents/carers	
Name of student:	
<p>When I use the school’s ICT facilities (like computers and equipment) and get on the internet in school :</p> <ul style="list-style-type: none"> ● I will not go onto a school computer, teacher’s phone or tablet, without permission from the teacher or other members of staff ● I will tell a teacher, or other member of staff, if I am uncomfortable with anything I see on a screen ● I will be kind and respectful to others if and when I am online, either when in or out of school 	
Signed (student):	Date:
<p>Parent/carer agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</p>	
Signed (parent/carer):	Date:



Appendix 4: Acceptable use agreement for Staff, Trustees, volunteers and visitors

Acceptable use of the school’s ICT facilities and the internet: agreement for staff, trustees, volunteers and visitors	
Name of staff member/trustees/volunteer/visitor:	
<p>When using the school’s ICT facilities and accessing the internet in school, or outside school on a work device, I will not:</p> <ul style="list-style-type: none"> ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) ● Use them in any way which could harm the school’s reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network ● Share my password with others or log in to the school’s network using someone else’s details ● Share confidential information about the school, its students or staff, or other members of the community ● Access, modify or share data I’m not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school 	
<p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.</p> <p>I will let the designated safeguarding lead (DSL) know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.</p> <p>I will always use the school’s ICT systems and internet responsibly and ensure that students in my care do so too.</p>	
Signed (staff member/governor/volunteer/visitor):	Date:



Appendix 5: Bring Your Own Device (BYOD) Agreement for Staff, Trustees, volunteers and visitors

Appendix 5: Bring Your Own Device (BYOD) Agreement for Staff

Name of staff member:

This agreement should be read and signed, in conjunction with:

- Acceptable Use (ICT) Policy
- Online Safety Policy
- Safeguarding Policy
- Use of Image Policy

The aim of this agreement is to define parameters and offer guidance with regards to the permitted use of own devices within school premises and, where appropriate, out of school premises i.e. whilst on a school trip.

1. Liability statement

I understand that LISAL is in no way responsible for:

- Personal devices that are broken while at school or on off-site school activities
 - Personal devices that are lost or stolen at school or on off-site school activities
 - Maintenance or upkeep of any device (keeping it charged, installing upgrades, fixing any software or hardware issues) – unless agreed with prior notification and request to the school for ICT assistance regarding the device
- Staff should ensure they have adequate insurance cover in place to cover the cost of repair/ replacement of a personal ICT device in the event of loss/damage.

2. School Guidelines for Responsible Use of BYOD

I understand that:

- Once on the wireless network, I have filtered internet access just as for any school owned device
- I am bound by the school's Acceptable Use Policy (ICT)
- Any digital images of students and staff which are present on the personal device are considered personal data and are covered by the Data Protection Act
- I will never use my personal device in non-communal areas, such as the toilet area
- I will use my personal device in the classroom only with permission of the DSL.



- I can use my personal device in the staffroom, office and non-teaching classrooms, providing I have read and understood the Acceptable Use (ICT) Policy and signed this agreement
- I understand that any ICT device should be used with care and the safety of staff and others on school grounds is paramount.
- I will take all sensible measures to protect information including, but not limited to, the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device).
- I will ensure my device will auto-lock if inactive for a period of time.
- I will never attempt to bypass any security controls in school systems or others' own devices.
- I will use the camera on my device in accordance to the relevant policies outlined at the outset of this agreement
- I will keep personal data and communications on their mobile devices separate from any school-related data
- I will hand over my personal device to the office staff if/when not in use

3. Monitoring and Enforcement of User-Owned Devices

I understand that:

- LISAL reserves the right to monitor the usage of staff members' own devices and to withdraw permission to access the school network for individuals or groups at any time
- The school also reserves the right to access staff-owned devices should there be a serious breach of this policy
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain inappropriate material including, but not limited to, those which promote pornography, gambling, violence, bullying or discrimination of any form.

4. Incidents and Response

I understand that:

- LISAL takes any security incident involving a staff member's personal device very seriously and will always investigate a reported incident.
- I will need to report loss or theft of the mobile device in the first instance.
- I will report Data Protection incidents immediately to the school's DSL.
- The school has the right to take action against anyone involved in incidents of inappropriate behaviour, outlined in our Whole School Behaviour and Online Safety and Acceptable Use (ICT) Policies.

5. Liability statement

I understand that LISAL is in no way responsible for:

- Personal devices that are broken while at school or on off-site school activities
- Personal devices that are lost or stolen at school or on off-site school activities



- Maintenance or upkeep of any device (keeping it charged, installing upgrades, fixing any software or hardware issues) – unless agreed with prior notification and request to the school for ICT assistance regarding the device
Staff should ensure they have adequate insurance cover in place to cover the cost of repair/ replacement of a personal ICT device in the event of loss/damage.

6. School Guidelines for Responsible Use of BYOD

I understand that:

- Once on the wireless network, I have filtered internet access just as for any school owned device
- I am bound by the school's Acceptable Use Policy (ICT)
- Any digital images of students and staff which are present on the personal device are considered personal data and are covered by the Data Protection Act
- I will never use my personal device in non-communal areas, such as the toilet area
- Only with the expressed permission of the DSL will I use my personal device in the classroom
- I can use my personal device in the staff room, office and non-teaching classrooms, providing I have read and understood the Acceptable Use (ICT) Policy and signed this agreement
- I understand that any ICT device should be used with care and the safety of staff and others on school grounds is paramount.
- I will take all sensible measures to protect information including, but not limited to, the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device).
- I will ensure my device will auto-lock if inactive for a period of time.
- I will never attempt to bypass any security controls in school systems or others' own devices.
- I will use the camera on my device in accordance to the relevant policies outlined at the outset of this agreement
- I will keep personal data and communications on their mobile devices separate from any school-related data
- I will hand over my personal device to the office staff if/when not in use

7. Monitoring and Enforcement of User-Owned Devices

I understand that:

- LISAL reserves the right to monitor the usage of staff members' own devices and to withdraw permission to access the school network for individuals or groups at any time
- The school also reserves the right to access staff-owned devices should there be a serious breach of this policy
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain inappropriate



material including, but not limited to, those which promote pornography, gambling, violence, bullying or discrimination of any form.

8. Incidents and Response

I understand that:

- LISAL takes any security incident involving a staff member's personal device very seriously and will always investigate a reported incident.
- I will need to report loss or theft of the mobile device in the first instance.
- I will report Data Protection incidents immediately to the school's DSL.
- The school has the right to take action against anyone involved in incidents of inappropriate behaviour, outlined in our Whole School Behaviour and Online Safety and Acceptable Use (ICT) Policies.

Signed (staff member):		Date:	
Device Type (phone/tablet/Laptop etc)	Device Make	Device Model (if known)	MAC Address
To obtain your MAC Address click on the link for instructions HERE			
Signed by Designated Safeguarding Lead:			