LANCASTER
STEINER SCHOOL

Acceptable Use Policy (ICT)

Version date: February 2020

Document review Period: September - November 2021

LANCASTER STEINER SCHOOL

CONTENTS

LANCASTER STEINER SCHOOL

1. INTRODUCTION AND AIMS

ICT (Information and Communication Technologies) is an integral part of the way our school works and is a critical resource for staff, Trustees, volunteers, parents and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, volunteers, Trustees, parents and pupils
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including Trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary procedures as outlined in the Employee Handbook.

Staff should read this policy in conjunction with the sections on Computer and Electronic Devices and Social Media Policy in the Employee Handbook. Other relevant policies:

- Online safety
- Safeguarding
- Whole School Behaviour
- Data protection
- Use of Image

2. RELEVANT LEGISLATION AND GUIDANCE

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006

- Keeping Children Safe in Education 2019
- Searching, screening and confiscation: advice for schools (updated version 2018)

3. DEFINITIONS

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including Trustees, staff, volunteers, contractors, visitors and – in some restricted contexts – pupils.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. UNACCEPTABLE USE

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms

This is not an exhaustive list. The school reserves the right to amend this list at any time. The designated Data Protection Officer and the DSL will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 EXCEPTIONS FROM UNACCEPTABLE USE

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the DSL and Data Protection Officer's discretion.

Approval will need to be requested in advance by emailing the DSL and/or Data Protection Officer with the request.

4.2 SANCTIONS

Staff, Trustees, volunteers and/or pupils who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Whole School Behaviour and Staff Disciplinary Procedures as outlined in the Employee Handbook, copies of which can be found in the School Polices' folder and in the HR cabinet.

5. STAFF (INCLUDING TRUSTEES, VOLUNTEERS, AND CONTRACTORS)

5.1 ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

The school's Data Protection Officer manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Data Protection Officer.

5.1.1 USE OF PHONES AND EMAIL

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Within their professional role, staff must communicate with parents. Trustees, volunteers and others using their work emails. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.2 PERSONAL USE

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Data Protection Officer may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action will be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Bring Your Own Device Agreement, found in Appendix 5.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 PERSONAL SOCIAL MEDIA ACCOUNTS

Members of staff should ensure that their use of social media, either for work or personal purposes, is always appropriate.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.4 SCHOOL SOCIAL MEDIA ACCOUNTS

The school has an official Facebook and Instagram page accounts, managed by the authorised personnel. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Professional judgement will be applied when deciding what can and cannot be posted on its social media accounts.

5.5 MONITORING OF SCHOOL NETWORK AND USE OF ICT FACILITIES

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business

- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. PUPILS

6.1 ACCESS TO ICT FACILITIES

Our school allows access to ICT facilities only during online safety curriculum sessions. In Class 5 pupils have access to devices but only under staff supervision and strictly as part of the online curriculum. In certain circumstances pupils with SEND may access assistive technologies, for example dictation software, under the supervision of a member of staff.

Pupils are not allowed to bring a mobile phone into school, unless in exceptional circumstances and with agreement with the school (see section Cameras, Mobile Phones and Devices in the Safeguarding Policy). However, were the need to search a pupil for a mobile device arise, DfE advice: Searching, Screening and Confiscation will be followed. A copy of this departmental advice is kept in the School's Safeguarding Portfolio.

6.2 SEARCH AND DELETION

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Whole School Behaviour if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community

- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. PARENTS

7.1 ACCESS TO ICT FACILITIES AND MATERIALS

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a Trustee) may be granted an appropriate level of access or be permitted to use the school's facilities at school's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Other authorised personnel will at times have access to the ICT facilities and materials, including the school's website, when requested to update those.

7.2 COMMUNICATING WITH OR ABOUT THE SCHOOL ONLINE

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. DATA SECURITY

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should always use safe computing practices.

8.1 PASSWORDS

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Parents or volunteers who disclose account or password information may have their access rights revoked.

The network administrator will allocate passwords for access to the network. This password will only change if it is compromised. Any suspected breach should be reported immediately to the School Manager, who will notify the administrator. The reason that the password is allocated is due to setting up the user on 5 different computers that are not linked to each other and each having to be configured for the individual by the network administrator. All passwords should be strong, individual and not be disclosed to anyone else. Any record of passwords must be kept securely and only accessed by the administrator if deemed absolutely necessary.

8.2 SOFTWARE UPDATES, FIREWALLS, AND ANTI-VIRUS SOFTWARE

All the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3 DATA PROTECTION

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

A copy of the Data Protection Policy can be found in the School Policies' Folder which is kept in the office.

8.4 ACCESS TO FACILITIES AND MATERIALS

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Data Protection Officer.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Data Protection Officer immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 ENCRYPTION

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the DSL.

For the use of personal device in relation to the capturing of images, please refer to our Use of Image Policy and the Bring Your Own Device Agreement in the Appendix.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as determined by the Data Protection Officer.

9. INTERNET ACCESS

The school wireless internet connection is secured.

There is a filter on the on the modem. Our filtering system is checked periodically – every term.

9.2 PARENTS AND VISITORS

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the school.

The school will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. MONITORING AND REVIEW

The DSL and Data Protection Officer will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The Board of Trustees is responsible for approving this policy.

LANCASTER STEINER SCHOOL

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

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page • Email/text groups for parents (for school announcements and information)	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • 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 I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers • 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.	
Signed:	**Date:**

LANCASTER STEINER SCHOOL

Appendix 2: Acceptable use agreement for Class 5 pupils only

Acceptable use of the school's ICT facilities and internet: agreement for pupils (Class 5) and parents/carers	
Name of pupil:	
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 (pupil):	**Date:**
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 pupils 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/carer):	**Date:**

LANCASTER STEINER SCHOOL

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

Acceptable use of the school's ICT facilities and internet: agreement for pupils (lower school) and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school : • 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 (pupil):	**Date:**
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 pupils 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/carer):	**Date:**

LANCASTER STEINER SCHOOL

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:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • 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 pupils 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	
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. I will let the designated safeguarding lead (DSL) and Data Protection Officer know if a pupil 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. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

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 Lancaster Steiner School 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 and Data Protection Officer
- 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:

- Lancaster Steiner School 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:

- Lancaster Steiner School 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 data protection officer.
- 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 Lancaster Steiner School 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
- I will use my personal device in the classroom, only with permission of the DSL and Data Protection Officer
- 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

7. Monitoring and Enforcement of User-Owned Devices

I understand that:

- Lancaster Steiner School 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:

- Lancaster Steiner School 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 data protection officer.
- 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 staff member is bringing into school:	
Signed by Data Protection Officer:	
Signed by Designated Safeguarding Lead:	