Camphill School Aberdeen

Acceptable Use of Information and Communications Technology (ICT) Policy for Camphill School Co-workers

Statement of policy and purpose of policy

CSA is committed to bringing the maximum benefits of ICT possible to its co-workers, and to equipping them with the knowledge, skills and attitudes that will enable them to thrive in the digital age. CSA provides co-workers with access to a range of communications and information technology equipment and systems (**resources**), both as a shared resource in the workplace and also through individual allocation of items for use inside or outside the workplace. It is our aim and responsibility to provide co-workers with all the resources necessary for the proper performance of their duties, in a reasonable and economical manner, and to ensure the security of resources against unauthorised access or abuse whilst ensuring their accessibility to authorised and legitimate users.

The purpose of this document is to explain to co-workers the standards we require them to observe in using our resources and the consequences of not adhering to these as well as to explain our policy in respect of monitoring use of our resources. This is a statement of policy only and does not form part of any contractual arrangement. CSA may amend this policy at any time, at its absolute discretion.

In accessing our resources, all co-workers will be deemed to have accepted the terms of this Acceptable Use Policy.

Scope

This policy and the rules contained in it apply to: all co-workers of CSA, irrespective of seniority, tenure and working hours, including all employees, long-term co-workers, volunteer co-workers, trustees, consultants and contractors, casual or agency co-workers and trainees.

The use of **CSA ICT Resources and BYODs** as in the definitions on pages 3-4 of the policy

Record of Approval				
1	***January 2016***	***Kathleen Scott***	***Norma Hart (for Board of Trustees)***	***January 2019***
Rev	***Date***	***Author***	***Approved***	***Review due***

Contents *Page*

1. Definitions and Abbreviations

CSA

Camphill School Aberdeen (Registered name: Camphill Rudolf Steiner Schools Ltd).

CSA ICT Resources

Computer servers and other hardware or equipment, desktop or portable computers, laptops, tablets and mobile telephones, Blackberries and other smartphones or personal digital assistants (PDAs), networks and systems, software, applications, subscriptions to databases and electronic resources, fax machines, scanners, printers, memory or storage devices, copiers, CCTV, electronic keys, passes and cards, routers, modems, PSTN line telephone equipment, PBX systems, network switches, PSTN lines, ISDN lines, ADSL internet connections, FTTC internet connections, Ethernet internet connections, physical LANs, Wi-Fi LANs, gaming platforms, photocopiers, digital cameras, external storage devices, email, the internet, and any data sent from, received by or stored on our computer or communications equipment or systems.

CSA Co-worker

Covers all employees, long-term co-workers, volunteer co-workers, trustees, consultants and contractors, casual or agency co-workers and trainees.

BYODs

Bring your own devices –any personal device that a co-worker uses to connect to any CSA ICT resource.

2. Introduction

The CSA Board of Trustees has overall responsibility for this policy and has appointed the CSA Finance Manager as the person with day-to-day responsibility for CSA ICT resources.

All co-workers have personal responsibility to use CSA ICT resources in a professional, ethical and lawful way, and to ensure compliance with this policy. All co-workers are expected to protect CSA ICT resources from unauthorised use or access at all times. Managers have special responsibility for leading by example, and monitoring and enforcing compliance.

A number of key factors should be used to inform judgement on whether a particular use of CSA ICT resources is acceptable or unacceptable:

- Cost - does the use involve significant extra costs to CSA, and if so are these outweighed by any benefits?
- Time - does this use impinge on work time?
- Acceptable content - does it comply with this policy?
- Legal and ethical issues - is the activity legal - is it ethical?
- Reputation - is it an activity that will bring CSA into disrepute?
- Compliance – does it comply with our other policies including, but not limited to, PVG Policy, Equality & Diversity Policy, Anti-Harassment/Anti-Bullying Policy, Data Protection Policy and Disciplinary Procedure?

Personal as well as business use of CSA ICT resources may be monitored and any breach of this policy will be taken seriously and may result in disciplinary action.

3. PC, Laptop and Tablet Use

3.1 Each CSA co-worker has responsibility for the appropriate use and day-to-day care of their office computer workstation and any computer equipment provided by CSA for use on or off CSA premises.

3.2 CSA co-workers may not connect personal equipment or peripherals, for example, flash memory cards and sticks, MP3 players, or digital cameras, to CSA business resources unless this has been authorised in advance by the Finance Manager.

3.3 CSA co-workers should log on to their workplace computer using an individual user name and password. CSA co-workers should not log on to any computer using someone else's name and password, or otherwise use our resources in a way that would lead us to believe that your activities are somebody else's, unless the Finance Manager has approved this in advance, even if you have the consent of the individual concerned.

3.4 CSA co-workers should ensure that their computer is not accessible to others when they are not in the vicinity of their computer. Screens should be locked or the machine logged out of whenever your computer is left unattended.

4. Mobile and Smartphone Use

4.1 Each CSA co-worker has responsibility for the appropriate use and day-to-day care of any mobile or smartphone provided by CSA for use on or off CSA premises.

4.2 CSA co-workers may not connect personal equipment or peripherals, for example, flash memory cards and sticks, MP3 players or digital cameras, to our resources, unless this has been authorised in advance by the Finance Manager.

4.3 CSA co-workers should ensure that their mobile or smartphone is locked with a unique PIN or password.

4.4 CSA co-workers should ensure that their mobile or smartphone is not accessible to others when not in their possession and that the device is locked.

5. Using Resources Outside Work

5.1 CSA co-workers authorised to use any resources away from CSA premises, including at home (remote resources), must take appropriate care of any equipment provided for this use, and ensure it is well maintained and used in accordance with CSA rules, including this policy and any specific instructions given by their line manager. Remote resources may be inspected without prior notice and, if requested, returned immediately for inspection or maintenance.

5.2 Remote resources provided are the responsibility of the co-worker who should take reasonable steps to ensure the security of equipment provided for use outside the workplace. When transporting equipment by car, it should be locked and left out of sight when the vehicle is unattended (e.g. in the boot).

5.3 Equipment and other resources for use outside the workplace are provided at CSA's discretion and can be withdrawn at any time. If requested, such resources should be immediately returned.

6. Personal Use of Resources

6.1 CSA resources are provided to support CSA co-workers in the proper performance of their duties. CSA co-workers may make personal use of resources, as long as all use complies with this policy and does not interfere with the proper performance of work duties or business use of the resources. However, in all cases, CSA co-workers should be aware that personal use of CSA systems may be monitored. Personal use of CSA resources is a discretionary privilege that we offer and which we may withdraw at any time, either in general or for particular co-workers. Co-workers who do not comply with our guidelines for personal use of resources or who otherwise abuse the privilege may have their right to personal use or access to certain

telephone numbers or Internet sites withdrawn, and/or disciplinary action may be taken.

7. Guidelines for Internet and Email Use

7.1 Email is an efficient and cost-effective means of communication and we encourage its appropriate use for business-related purposes. However, inappropriate or negligent use of email carries significant risks.

7.2 Communications by email, like all other modes of communication, must not breach CSA disciplinary or workplace rules or any other policy and procedure, and must not cause CSA to be in breach of obligations we owe to others. See the Misuse of Resources section of this policy, below, for further information.

7.3 Confidentiality is a particular concern when using email. CSA co-workers must be careful in addressing messages to make sure that communications are not inadvertently sent to unintended recipients. In addition, although we take steps to protect data security, you should be aware that the confidentiality of data (including email messages) sent via the Internet cannot be assured. You should only send sensitive information belonging to or relating to third parties or us to whom we have obligations of confidence and duties of care when it is absolutely necessary to do so and in line with our guidelines.

7.4 Delivery of email cannot be guaranteed. It is important to check that urgent or important emails have arrived safely with the intended recipient.

7.5 In general CSA co-workers should not distribute chain mail, junk mail, jokes or gossip, trivial or unnecessary messages, or agree to terms, enter into contractual commitments or make representations by email unless you are authorised to do so.

7.6 Emails received in error should be deleted and the sender should be notified. The contents of an email received in error should not be disclosed.

7.7 Attachments or links sent by email may contain viruses. While CSA takes measures to protect against viruses, emails, attachments or links should not be opened unless they are from a source that is known and trusted. Any virus alert or notification should be reported immediately to the Finance Manage.

7.8 When using email, CSA co-workers should observe the standards for communication that CSA expects for other forms of writing, including style, content and choice of language.

7.9 Consideration should be given as to whether there is a more suitable method of communication, for example where there is a need to preserve confidentiality or in the case of sensitive issues, which should be communicated face-to-face.

7.10 Judgement and discretion should be used when considering using a work email address to register or sign up for online services or otherwise to communicate with any provider of goods or services, since this is likely to increase the amount of spam email that CSA receives.

7.11 CSA co-workers must comply with any guidelines that we issue concerning filing, archiving and deletion of emails.

7.12 When out of the office on a working day an automated 'out of office' message should be created to alert correspondents to your absence and the arrangements for dealing with any urgent queries.

7.13 Encryption software allows messages sent between communication devices to be encoded in such a way that third parties cannot read them. In some cases, for example when securely sending credit card details, this can happen automatically. In others, such as the sending of email, the sender actively invokes it. Messages should only be encrypted using engager-approved software and only where this is required for purposes of confidentiality. Engager email systems must not be used for the sending of confidential private messages and non-approved encryption software must not be used in order to achieve confidentiality.

7.14 When using the Internet, co-workers should observe netiquette (online etiquette) as appropriate to the systems they are using and to avoid causing offence to other users.

7.15 Viruses can be transferred between computers, either over the Internet or by using USB drives or other media between machines. All co-workers should ensure that their devices are properly protected from virus infection and that they take action to ensure that viruses are not passed from home or other devices to those of CSA. Co-workers should also encourage others in their care to adopt sensible practices when using both CSA devices and those they have access to at home.

7.16 Each Internet site visited has the ability to detect information about the user, including CSA's identity as an organisation and potentially that of the user. Third parties, anywhere in the world, may access the information that is input on an Internet site. Accordingly, judgement and discretion should be used in determining the Internet sites that users choose to access and the activities on those sites.

7.17 Internet systems are very effective at hiding the true identities of users from each other. This accounts for some of their appeal, allowing as they do, the adoption of different personae and the ability to communicate openly in relative anonymity. This and other characteristics of the Internet do, however, open the way for various kinds of abuse. Co-workers must ensure that they and others in their care are aware of the dangers of using the Internet, and are equipped with strategies for avoiding them (e.g. not handing out personal details to strangers on the Internet).

7.18 You must read and comply with the terms and conditions of any Internet site that you access using CSA resources.

7.19 Copyright issues as they relate to the Internet are in flux. Copyright as it applies to the Internet should be seen as being more stringent than that applying to other media. There are no special arrangements relating to the Internet which extend co-workers' copying rights beyond those allowed by general copyright law, nor do general copyright agreements entered into by CSA currently extend to materials on the Internet. It is safest to assume that, unless otherwise stated on the web pages concerned, copies (whether paper-based or electronic) cannot be made. If users wish to make use of pages that will involve any kind of copying, the best approach is to email the copyright holder and ask for permission. However, when using Internet

pages, it is good practice to use a link to the site rather than attempting to copy pages. Clarification on copyright issues can be sought from the Finance Manager.

7.20 Mailing lists, newsgroups and blogs are useful for the exchange of information and ideas. They can also contribute to professional development. When using such systems, however, it must be borne in mind that they are essentially public spaces and that contributing to them may have legal repercussions. Therefore, when using these systems, co-workers should use a signature file or other disclaimer, indicating that any views expressed are their own and not the official view of the engager. It should be recognised, however, that the use of an engager email address, and the fact that a contributor is a Camphill School co-worker, implies a degree of official status. The use of such a signature file does not, therefore, release co-workers from their obligations under this policy.

7.21 While the bulk of current use of social media is recreational, these systems can have considerable potential in collaborative learning and working. When using such systems, however, it must be borne in mind that they are essentially public spaces and that contributing to them may have legal repercussions. Personal use of social media by co-workers during working hours is permitted as long as it does not involve unprofessional or inappropriate content, does not interfere with your engagement responsibilities or productivity, and complies with this policy.

7.22 Making personal credit or debit card purchases over the Internet will be acceptable as long as CSA is not being used in any way to imply the official status of the purchaser. However, using CSA resources to run a non-engager business, for example, is clearly unacceptable.

7.23 Co-workers must:

- **not** disable, alter settings or interfere in any way with any measures implemented by us to ensure the security of resources and/or avoid computer viruses in connection with Internet use, including our firewall arrangements
- **not** visit any inappropriate Internet site, including any Internet site that is offensive, insulting, discriminatory or obscene, or is likely to damage your reputation or that of CSA
- **not** engage in illegal file sharing
- use judgement and discretion when downloading any program, data, game or other material from the Internet, without the prior approval of the Finance Manager, because of the prevalence of viruses on the Internet. Users are expected to take reasonable steps to ensure that they are downloading from a trusted and reputable source
- when downloading files for personal use, ensure that they do not compromise the security or performance of either the machine which they are using or CSA resources as a whole. Specifically, users must manage their personal files so as not to take up excessive storage space on the device they are using or on engager servers. This can be done by moving them to personal media such as a USB flash or external HDD drive
- acknowledge that CSA cannot guarantee the security of any data stored on local machines. CSA reserves the right to open any data or files stored on local hard drives or otherwise on the network. Co-workers are responsible for their own back-ups in respect of any personal data or files that are important to them. CSA takes no responsibility for any data loss or damage

to any media used on our resources such as, but not limited to, CDs, DVDs and USB drives.

8. Guidelines for Software Use

8.1 Most of the software and applications we use are licensed from third parties and our use is subject to terms and conditions. CSA co-workers must always comply with the terms of any software licence we hold. Any software or application you copy, download or install without the prior approval of the Finance Manager will be subject to this policy.

8.2 If any computer, phone, or other hardware provided to you by CSA prompts you to update or renew any software or application licensed to CSA, then you must do so promptly, unless we have told you not to. Where support is required for this purpose, please refer to the Finance Manager.

9. Monitoring of Use of CSA Resources

9.1 CSA may monitor and intercept the use of CSA resources, including Internet use and communications sent to or received by CSA co-workers by phone, email (including associated files or attachments), fax or any other means involving our resources, for a number of relevant business reasons, including but not limited to:

- ensuring compliance with the terms of this policy
- training and monitoring standards of service
- ensuring compliance with regulatory practices or procedures imposed or recommended by any regulatory body relevant to our business
- ascertaining whether internal or external communications are relevant to our business
- preventing, investigating or detecting unauthorised use of our IT systems for criminal activities
- maintaining the effective operation of our resources - in particular all emails received by the engager are automatically scanned for viruses
- establishing the existence of facts.

9.2 Where it becomes apparent in the course of monitoring emails or other communications that a particular message is obviously private, CSA will take reasonable steps to respect co-worker privacy in respect of that message. However, it may not be possible to determine whether that communication is personal or business related until it is already open and read. CSA co-workers should have a reasonable expectation of privacy as to their use of CSA resources, including communications sent or received by phone, email (including associated files or attachments), fax or any other. To maintain complete privacy of communications, CSA resources should not be used for personal use.

9.3 Certain authorised co-workers involved in administering our resources may necessarily have access to the contents of email messages in the course of their duties. Any knowledge thus obtained should not be communicated to others, unless necessary for legitimate business reasons.

9.4 CSA may also take any action in administering email or other communications that is reasonably necessary to preserve the integrity or functionality of CSA resources including as part of a firewall or spam or virus protection arrangements. This could include the deletion or non-transmission of any emails or communications (including any personal communications).

10. Password Policy

10.1 Appropriate passwords are vital to maintaining the security of CSA resources.

In general, to access certain resources such as computers, mobile phones or other devices or certain information sources or accounts, it will be necessary to enter a password or personal identification code. Passwords should be kept private and are the direct responsibility of the person to whom the account or device is allocated. Where access to any device or equipment that CSA provides can be secured by a password or code, that facility must be used.

10.2 **Password standards**

Passwords used on CSA resources should adhere to the following standards, where permitted by the device or account in question:

- They must contain at least 8 characters in total and at least one of each of the following: uppercase character, lowercase character and numeric character.
- Reasonable efforts should be made to ensure it is not a dictionary word in any language, slang, dialect, jargon, etc.
- They should not be based on readily available information such as date of birth, spouse's or child's name, telephone numbers or address.
- They should not be the same as or contain your name or username.
- Password should not be the same as those used for personal accounts or devices.
- They must differ from previous passwords.

10.3 **Password security**

- CSA co-workers are personally responsible for maintaining the security of their passwords used on CSA resources. Co-workers must not disclose their password to anyone else, inside or outside Camphill School Aberdeen, except as directed by the Finance Manager. You may not keep a record of your passwords anywhere on our premises or any device unless it has been encrypted.
- No attempt should be made to access any restricted area of CSA resources or to guess or determine the password of any other user.
- Device passwords or other access codes must be changed when prompted to do so either automatically or by the Finance Manager or, if sooner, every 90 days.
- If a CSA co-worker is aware or suspects that another person knows his/her password, then the password should be changed immediately and the Finance Manager notified of the situation.
- On termination of a CSA co-worker engagement, however arising, or if requested to do so by the Finance Manager, the co-worker should provide details of all passwords used on our resources to the Finance Manager.

11. Misuse of Resources

11.1 The same principles apply to the use of resources for communication, including through email, telephone and the Internet, as apply to any means of communication and you must not use these for any purpose or in any way which could be subject to disciplinary or legal action in any other context. In particular, you must not use CSA resources in any way that:

- breaches obligations of confidentiality which you owe to us or to any third party or which causes us to breach duties of confidence which we owe to any third party
- breaches the rights of any other co-worker's privacy, data protection and confidentiality or which amounts to bullying or harassment
- is offensive, insulting, immoral, discriminatory, obscene, pornographic or sexually explicit
- poses a threat to our confidential information and intellectual property
- infringes the intellectual property rights of any other person or entity
- defames or disparages us or our associated companies or any party with whom we have a business relationship, such as suppliers or customers
- includes information which may be, or could reasonably expected to be, subject to provisions of counter-terrorism legislation
- breaches or causes us to breach any law or the rules or guidelines of any regulatory authority relevant to our business
- breaches data protection rules
- breaches our rules, policies or procedures for the use of our ICT systems or other equipment or resources
- is dishonest, improper, unethical or deceptive (e.g. pretending to be someone or attempting to access another employee's computer, computer account, email, files or other data)

- is likely to damage your reputation or that of Camphill School Aberdeen
- wastes resources or use them excessively or to the exclusion of others
- interferes with the work of others or our computer, technology or communications systems
- includes any other statement which is likely to create any criminal or civil liability (for you or us)

Further, CSA co-workers must not:

- delete, destroy or attempt to modify our resources or any information contained on them except in line with this policy or instructions given by the Finance Manager
- use our resources to conduct any business other than CSA business

It should be noted that the following activities are criminal offences: unauthorised access to computer material (hacking); and unauthorised modification of computer material.

Any such action will be treated very seriously and is likely to result in summary dismissal. Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. Any information obtained may be handed to the police in connection with a criminal investigation.

A number of activities related to the use of the Internet or email are covered by law, by other organisational policies or regulations, and are otherwise clearly unacceptable. These will be regarded by the engager as constituting misconduct and any co-worker involved will be subject to disciplinary action up to and including dismissal. These include: terrorist activities, on-line stalking, grooming, Internet luring, soliciting of children by computer, defamation, retention of offensive screen savers, fraud, software theft, damage to engager systems, retention of other people's personal details/information, drug-related activities, or any other illegal activity.

In addition, Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on the engager to have, in the exercise of its functions, due regard to the need to prevent people from being drawn into terrorism. This means that the engager will place an appropriate amount of weight on the need to prevent people being drawn into terrorism in the application of this policy.

12. Guidelines for Use of BYODs

12.1 CSA recognises that co-workers may wish to use their own personal ICT equipment while on CSA premises and may also wish to connect to CSA networks.

This is a trend, which CSA views as positive and which it seeks to encourage through the use of support for BYODs. At the same time, this brings with it certain risks, including security risks, which must be effectively managed.

In order to do this, and to comply with current legislation, anyone wishing to use their personal device must sign and return the declaration at the end of the policy and the following will apply:

- At all times when any device is connected to CSA networks or power supplies, it must be used only in accordance with all CSA policies and regulations, and the instructions of CSA.
- Where a device is to be connected to CSA power supplies, whether for use or for recharging, the device must be EITHER i) less than 3 years old OR ii) PAT tested. Users should only connect to the engager's power supplies which are indicated by the line manager as being available for this when this can be done in a way which is compatible with the health and safety of all, and does not create any kind of hazard. Care must be taken, for example, to ensure that there are no trailing cables, which might create a trip hazard. Where PAT testing is required, it is the responsibility of the owner of the equipment.
- No device should be connected to CSA networks, whether wirelessly or in any other way, with any malicious intent, or for any purpose incompatible with the engager's role as a charitable company provider of care and education (it should not be for any commercial purpose, for example, or with the aim of deliberately damaging the network).
- The user of any personal device must take all reasonable steps to ensure that the use of their device does not compromise or damage the engager's network in any way. They must ensure, for example, that proper virus protection is installed and used on the device.
- The user must at all times use their best efforts to physically secure the personal device against loss, theft or use by persons who the engager has not authorised to use the device, and protect the device with a pin or password. If the security of the device is compromised, this should be reported to the Finance Manager immediately.
- All devices are connected to CSA's power supplies or networks entirely at the user's own risk. In agreeing to the terms of the CSA 'Declaration and Agreement – Acceptable Use,' users agree that the engager will not be responsible for any loss, damage to the device, or damage to or corruption of data held on the device and/or liability arising out of its use which results from such connection.
- Users should make use of the normal facilities provided by CSA for access to CSA networks by user-owned devices. They should not seek to access the network, circumvent security processes or bypass network access controls that are in place. Specifically, they should not seek to 'hack' into the network in any way whether for malicious or other intent, attempt to bypass Internet access controls, or hide activities, e.g. by the use of proxy services.
- Where damage to the CSA network, power supply or other infrastructure occurs through negligence or malice on the part of the device user, or through failure to comply with engager policy and regulations, the user will be held liable for the damage caused. Such a situation would arise, for example, where damage results relating to: a device which is more than 3 years old and has not been PAT tested; malicious infection of the engager network with a virus; accidental infection of the engager network with a virus where appropriate measures have not been taken to prevent this; damage caused through unauthorised access to the engager network, i.e. hacking (this list is not exhaustive).

- Use of the CSA network to facilitate threatening, intimidating or abusive behaviour towards another person, even via privately owned devices, shall be deemed to be a breach of the Acceptable Use Policy and the Bullying Policy. In such cases appropriate action will be taken in accordance with the Co-worker Disciplinary Policy.
- CSA reserves the right to refuse or remove permission for a user's device to connect with engager's systems.
- All materials, data, communications and information created on, transmitted to, received or printed from, or stored or recorded on a personal device during the course of business or on our behalf is our property, regardless of who owns the device.
- CSA reserves the right to monitor, intercept, review and erase, without further notice, all content on the personal device that has been created for CSA or on our behalf, as well as inspect the device. Users must co-operate with CSA to enable such inspection, access and review, including providing any passwords or PIN necessary to access the personal device or relevant applications. A failure to co-operate with CSA in this way may result in disciplinary action being taken, up to and including dismissal.
- It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, you should have reasonable expectations of privacy (see Section 9.2) in any data held on the personal device if used for business purposes. Co-workers are advised not to use our ICT systems for any matter that they intend to keep completely private or confidential.
- Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including (but not limited to): in order to prevent misuse of the personal device and protect engager data; ensure compliance with our rules, standards of conduct and policies in force from time to time (including the Acceptable Use Policy); monitor performance at work; and ensure that co-workers do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

12.2 By agreeing to the terms of the engager's 'Declaration and Agreement – Acceptable Use', you confirm your agreement (without further notice or permission) to such monitoring and to our right to copy, erase or remotely wipe the entire personal device (including any personal data stored on the device).

On the last day of engagement as a Camphill School co-worker, all engager data (including work emails) and any software applications provided by us for business purposes, will be removed from the personal device. If this cannot be achieved remotely, the device must be submitted to the Finance Manager for wiping and software removal. You must provide all necessary co-operation and assistance in relation to this process

13. Other Relevant Policies

Co-workers are referred to the co-worker policies and procedures which may be relevant to the issues covered in this policy:

Bullying and Harassment Policy

Disciplinary Policy

SSSC Code of Conduct

14. Declaration

PART 1: to be retained by the co-worker

This declaration refers to the Camphill School Policy on the Acceptable Use of Information and Communications Technology (ICT), and confirms that you have been provided with a copy and that you have agreed to adhere to the contents. All co-workers are required to familiarise themselves with the contents of the policy and sign the following declaration.

Declaration

You should sign two copies of this document; this copy is to be retained by you. The second copy (below) is to be detached and placed in your personal file.

I confirm that I have been provided with a copy of the school's policy on the Acceptable Use of Information and Communications Technology (ICT). I confirm that I am aware of the contents of the policy and agree to comply with the contents of the policy.

Signed: ..... Name: ..... Date: .....

PART 2: to be detached and kept by school

This declaration refers to the Camphill School Policy on the Acceptable Use of Information and Communications Technology (ICT), and confirms that you have been provided with a copy and that you have agreed to adhere to the contents. All co-workers are required to familiarise themselves with the contents of the policy and sign the following declaration.

Declaration

You should sign two copies of this document; this copy is to be retained by you. The second copy (below) is to be detached and placed in your personal file.

I confirm that I have been provided with a copy of the school's policy on the Acceptable Use of Information and Communications Technology (ICT). I confirm that I am aware of the contents of the policy and agree to comply with the contents of the policy.

Signed: ..... Name: ..... Date: .....