Destiny House International and DHI Education and Arts

IT, Social Media & Communications Policy

Contents

1. Policy & Purpose

IT, Social Media and communications are integral to how we run Destiny House International CIO referred to as 'the Church'.

While we operate a strong culture of trust regarding email, social media, and internet access, we also need to ensure we set reasonable parameters for using them so that everyone who uses our IT infrastructure and/or equipment is clear and can work within them.

Use of the Church's email and internet is provided during working hours for effectively completing work, and use must comply with all Changing Lives policies and procedures.

This policy applies to everyone who uses the Church's IT infrastructure (including social media accounts) and/or equipment, and the aim of it is to explain acceptable email, social media, and internet use.

2. Key points to remember

You must use our IT and communications facilities (including social media accounts) sensibly, professionally, lawfully, and consistently with your duties and in accordance with this policy and other Church rules and procedures.

You must always behave with honesty and integrity and respect the rights and privacy of others in relation to e-communication and information.

All employees will be given internet access and access to the Church's IT systems.

All PC/network/social media access will be through passwords; no one is allowed onto the system using another employee's password. Employees must not share their password with anyone inside or outside of the Church. Passwords must not be kept in plain sight at any time (attached to laptops or monitors) and should not be attached to the underside of monitors or keyboards. You can set your own password, and they must be changed often, prompted by the reminders. Passwords must be shared with the trustees by forwarding them to the central email provided. The trustees will respect privacy in line with GDPR guidance by ensuring sensitive information is viewed on a need-to-know basis.

All information relating to the Church's operations is confidential. Therefore, you must treat our paper-based and electronic information with utmost care.

Many aspects of communication are protected by intellectual property rights, and these can be infringed in several ways: downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other IP rights.

If you are contacting others using e-mail, think about what you write as the content may bind you and/or the Church and can be produced in court in the same way as other kinds of written statements.

3. Personal use of email, internet & social media

While we may give you access to e-mail, the internet, and social media for business use, we understand that you might want to use them occasionally for personal use, within reason.

Your work email address should not be used to send personal emails.

4. Unauthorised use of email and internet

The Church will not tolerate the use of email and the internet for unofficial or inappropriate purposes, including:

- any messages that could constitute bullying, harassment or other detriments
- online gambling
- accessing or transmitting pornography
- accessing other offensive, obscene or otherwise unacceptable material
- transmitting copyright information and/or any software available to the user
- posting confidential information about other employees, the Church or its customers

5. Downloading of material

So that we can protect our systems, you must ensure the following:

- unauthorised software, including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads, is not to be used, and
- all software must be virus checked by the Church using standard testing procedures before being used.

6. Social Media Use

This means profile pages and other resources you may use on networking sites including, but not limited to, Facebook, Twitter and LinkedIn, as well as blogs, forums, message boards, review sites and online polls.

While Social Media can be a great tool, it can also be distracting and have a negative effect on your work. It's important that when it is used at work, it is used in a way that does not negatively affect the Church's reputation.

This area applies to all social media users, either for personal or professional reasons. Social media may blur the boundaries between what is at home and work. Access is often public, even amongst a limited group of connected accounts, and comments are often permanent.

We ask you to be honest and respectful when using social media and remember that everything posted on there may be tracked back to the source. All content posted on social media accounts, both in work and personal capacity, must fit with the Church's vision, values, ethos, CSR and marketing brands.

7. When can I use it

Social media usage for work purposes is limited to individual roles and, unless part of your job description, needs to be approved by a senior manager.

Social media usage for personal reasons does not need approval by the Church.

When using social media, either in a personal or work capacity, during or outside working hours, posting on social media must not:

- compromise the Church, disclose confidential data or disclose sensitive data
- must not damage the Church's reputation or brand
- must not breach the copyright or data protection
- contain libel or defamatory content
- must not engage in bullying or harassment
- be of illegal, sexual or offensive content
- interfere with your work commitments
- use the name of the Church to promote products or political opinions.

Social media content from you which breaches the terms of this policy, or the other related policies, may result in an investigation and disciplinary action under the Church's disciplinary policy.

8. Networking & Blog use

We believe that these can be an effective and useful way of communicating, but there is the potential for misuse during and out of work hours.

We have therefore put the following guidelines in place:

- to help protect the Church against potential liability
- to give you clear guidance on what can and cannot be said about the Church or other workers
- to help managers effectively manage employee performance, time management and use of the Church's resources
- to help you separate your professional and personal communication
- to comply with the law on discrimination, data protection, and to protect the health and well-being of employees
- to be clear about the use of monitoring within the Church

You must not use an online blog or social networking site for unofficial or inappropriate reasons unless this has been authorised and approved specifically:

- You should not at any time upload photographs to your social networking sites of yourself or any other employee taken in a work situation without consent. No defamatory comments about the Church should be made on such sites at any time.
- You should not at any time include information that identifies any other employee/volunteer/member of the public or any other individual working in connection with us.
- You should not at any time express opinions on such sites which purport to be the opinion of the Church, nor comments representing your own views on our Church.
- Any personal blogs should contain a disclaimer that the views expressed on them are the author's personal views only.
- You should not at any time make comments on such sites which bring the Church into disrepute.
- You should not reveal confidential church information or information on clients/customers/suppliers etc.
- You should not at any time make comments on such sites which amount to bullying, harassment or any other detriment towards other employees/volunteers/members of the public or any other individual working in connection with us.

We advise you to use strict privacy settings on your social network profiles.

The term "use" includes accessing social media by means of a PC, mobile phone or any other device.

9. Monitoring

In order to comply with our own legal obligations, the use of our IT and Communications resources, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent allowed or required by law and as necessary and justifiable for business purposes.

We reserve the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

- to monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;
- to find lost messages or to retrieve messages lost due to computer failure;
- to assist in the investigation of alleged wrongdoing; or
- to comply with any legal obligation.

Misuse or excessive use or abuse of our telephone or email system or inappropriate use of the internet in breach of this policy will be dealt with under our disciplinary procedure.

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. If necessary, such information may be handed to the police in connection with a criminal investigation.

10. Misuse

Any employee who we suspect has breached this policy will be subject to the Church's disciplinary procedure.

11. Storage of emails

You should regularly review your emails to archive or delete those that contain information that is no longer required for DHI to comply with its obligations under the General Data Protection Regulations and Data Protection Act 1998.

Unless you are responsible for the upkeep of the Church's website as part of your role, you are not permitted to add anything to the website without the express permission of a manager.

12. Use of IT equipment

DHI will provide you with all hardware and software equipment required for the performance of your role.

The following rules apply to the provision of this equipment:

- You must take all due care when operating the equipment, making sure that no drinks are left near electrical items and that no unauthorised person is using DHI equipment.
- If your work location is your home address, please ensure that your home and contents insurance is extended to cover work-related materials.
- You should not regard DHI property provided for your use as your own. It must be returned when you leave our employment or at other such time as directed by DHI.
- The responsibility for the upkeep of the equipment and any liability or risks associated with the use of the equipment for DHI -related business purposes remain with you

13. Mobile phones

When necessary, DHI will provide our employees with the use of a mobile phone to enable them to carry out the responsibilities of their roles.

The mobile phone is primarily for business use, although a limited number of essential and necessary personal calls are permitted. Any costs considered excessive will be expected to be reimbursed by the employee.

Mobile phones will only be upgraded if they are on a monthly contract and eligible for an upgrade.

14. Using Devices Remotely

Special care needs to be taken when using any portable device or remote electronic devices outside work for work-related matters, as such devices may contain confidential or personal information. This could include the use of our or your own laptop, your home computer or mobile phone. Sensitive data should not be stored on a USB flash drive.

If you use such a device for work-related matters, you should ensure that:

- It is stored safely at all times and is password protected
- confidential information stored on the device is not visible to people around you
- if the device is lost or stolen, notify the police and your manager immediately.

If you have any questions regarding IT equipment or mobile phones, please contact the IT department.

15. Breach of this policy

Failure to follow this policy may be viewed as a breach of the Church's disciplinary rules and will be dealt with under our disciplinary procedure. It may also lead to your access to the Church's systems on your own device to be prohibited and may also result in disciplinary action or dismissal.

If there is anything in this policy that you do not understand, please discuss it with your line manager.

Approved by:	DHI CIO Board of Trustees
Last reviewed on:	September 2022