APPROPRIATE AND SAFE USE OF IT AND SOCIAL MEDIA POLICY

1. Introduction

The aim of this policy is to ensure that cHRysos HR's IT facilities and social media platforms are used safely, lawfully and equitably.

cHRysos HR seeks to promote and facilitate the proper and extensive use of IT and social media in the interests of learning, teaching and research and in the day to day undertaking of tasks. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to learners/apprentices, staff and associates.

This policy describes the rules governing IT and social media use at cHRysos HR. It also sets out how staff, associates and learners/apprentices are expected to behave when using IT/social media.

2. Scope

This policy applies to all computing, telecoms, cloud systems and social media platforms provided within the organisation and should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to in this policy.

This policy applies to anyone using cHRysos HR IT facilities (hardware, software, data, social media platforms, services provided by licensed third parties or online cloud services including learners, apprentices, staff, associates, and third-party individuals who have been given access for specific purposes.

It applies no matter whether IT, cloud-based systems, social media is being used while homeworking, while travelling for business and to any device owned by cHRysos HR or connected to cHRysos HR's systems.

cHRysos HR facilities may be accessed via company-owned devices or via personally owned devices but only with prior authorisation. Where IT e.g., laptops are provided these must be used for work purposes.

.

3. Acceptable use

cHRysos HR recognises that the use of IT, the internet, social media and other technology is an integral part of studying and doing business. The company therefore encourages use whenever this supports learning or the achievement of cHRysos HR goals and objectives.

cHRysos HR resources are provided primarily for academic and operational purposes to support learning and teaching, research, enterprise and the day-to-day business of the company. Facilities are also provided to enhance the wider experience of those studying or undertaking an apprenticeship with cHRysos HR.

Whilst the principles of academic freedom will be fully respected, facilities must be used responsibly, in accordance with the law and not to bring cHRysos HR into disrepute.

Personally owned devices whether owned by learners, apprentices, staff or associates must be maintained with up-to-date anti-virus software.

Use of the facilities for personal activities is permitted but this is limited to the internet or cloud-based applications/systems. This is only provided that it does not infringe the law or cHRysos HR policies, does not interfere with others' valid use and, for staff, is not done inappropriately during their working hours. You must not download and/or store personal use documents ore use external USB devices in any company-owned equipment e.g., laptops.

Use for personal activities may be withdrawn if it is not in accordance with this policy.

You must not use company-owned equipment for commercial work for outside bodies, that is being undertaken on a personal basis, solely for personal gain and not on behalf of cHRysos HR unless prior permission has been sought from the Managing Director or Director-owner.

cHRysos HR e-mail addresses and associated systems must be used for all official cHRysos HR business, to facilitate auditing and record keeping. All staff and associates must regularly read their own @chrysos.org.uk and/or @chrysoshr.org.uk e-mails, put out of office notification on emails if they are to be absent for more than 1 day.

Out of office notification must include contact details for an alternative member of staff in their absence and contact details for the cHRysos HR's Safeguarding lead and deputies.

When using cHRysos HR's IT facilities and social media, you remain subject to all relevant laws and policies, and, when accessing services from another legal jurisdiction, you must abide by all relevant laws, as well as those applicable to the location of the service.

Following the requirements of this policy, and other cHRysos HR policies and procedures applicable to your activities, should normally ensure that you comply with the law.

You must abide by the policies and terms and conditions applicable to any other organisation whose services you access. When using cHRysos HR IT services from another institution or company, you are subject to both cHRysos HR's requirements and those of the institution or company where you are accessing services.

Any licence conditions must be adhered to when using software procured by cHRysos HR.

Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

4. IT Security and Passwords

Only those who have been authorised to use cHRysos HR's IT facilities and software may do so.

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorised access to our most sensitive data and/or exploitation of our resources. All staff, including associates with access to cHRysos HR systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

You must take all reasonable precautions to safeguard your username, password and any other IT credentials issued to you.

You must not allow anyone else to use your IT security credentials. No-one has the authority to ask you for your password, and you must not disclose it to anyone unless requested to do so by the Managing Director or Director-Owner.

You must not attempt to obtain or use anyone else's security credentials; and you will be held responsible for all activities undertaken using your IT security credentials. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

4.1 **Password Creation and Use**

All user-level and system-level passwords must conform to the Password Construction Guidelines.

Users must use a separate, unique password for each of their work-related accounts. Users should not use any work-related passwords for their own, personal accounts.

Staff are only allowed to use authorised, approved password managers to securely store and manage all their work-related passwords.

User accounts that have system-level privileges must have a unique password from all other accounts held by that user to access system-level privileges. In addition, wherever available some form of multi-factor authentication must be used for all accounts.

4.2 **Password Change**

On occasion cHRysos IT administrators will apply a forced password change and this must be complied with on all accounts, as directed.

4.3 Password Protection

Passwords must not be shared with anyone, including managers and coworkers. All passwords are to be treated as sensitive and confidential cHRysos HR information.

Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

Passwords may be stored only in password managers authorised by the organisation.

Do not use the "Remember Password" feature of applications (for example, web browsers).

Any individual suspecting that their password may have been compromised must report the incident to the Managing Director or Quality Lead (in their absence) and change all relevant passwords immediately.

4.5 Multi-Factor Authentication

Multi-factor authentication is mandatory if available.

5. Policy Compliance

Compliance Measurement: cHRysos HR IT administrators will verify compliance to this policy through various methods, including but not limited to internal and external audits, and feedback to the Managing Director

5.2 Exceptions

Any exception to the policy must be approved by the Managing Director or Director-owner in advance.

5.3 **Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment depending on the severity of the breach.

6. Anti-virus guidelines

Always run the recommended, supported anti-virus software available. Download and run the current version.

Download and install anti-virus software updates as they become available.

Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.

Delete these attachments immediately, then "double delete" them by emptying your Trash/Deleted items. Delete spam, chain, and other junk email without forwarding.

Never download files from unknown or suspicious sources.

Avoid direct disk sharing with read/write access unless there is an authorised business requirement to do so.

Periodically check that your anti-virus is working correctly and ensure that there are no programs running on your system require any attention e.g., outdated software.

Internet security

Used unwisely, the internet can be a source of security problems that can do significant damage to company data and reputation.

Users must not knowingly introduce any form of computer virus, Trojan, spyware or other malware into the company.

Employees, associates, learners and apprentices must not gain access to websites or systems for which they do not have authorisation.

Security of the company's systems and data must always be considered when using the internet. If you need help and guidance, please ask the third-party IT support company.

6. Blogging and Social Media

Blogging or posting to social media platforms by employees and associates, whether using cHRysos HR's property and systems or personal computer systems, is also subject to the terms and restrictions outlined in this Policy. Limited and occasional use of cHRysos HR's systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate cHRysos HR's policies, is not detrimental to our best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from cHRysos HR's systems is also subject to monitoring.

Employees are prohibited from revealing any cHRysos HR confidential or proprietary information, trade secrets or any other material when engaged in blogging and other social media activity.

Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of cHRysos HR and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by cHRysos HR's Equality, Diversity, Harassment and Bullying policy.

Employees or associates may also not attribute personal statements, opinions, or beliefs to cHRysos HR when engaged in blogging or other social media activity. If an employee or associate is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of cHRysos HR. Employees assume any and all risk associated with blogging or similar social media activity.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, cHRysos HR's trademarks, logos and any other intellectual property may also not be used in connection with any blogging or social media activity.

All employees, learners (including apprentices) and associates must follow the guidance under section 8 below titled Behaviour.

7. Data protection and illegal downloading

You must make yourself aware of cHRysos HR's Data Protection Policy and take all reasonable steps to safeguard any information you have access to in accordance with the law.

You must not infringe copyright or break the terms of licences for software or other material. If in doubt, please contact the Business Support/Marketing Officer.

You must not attempt to access, delete, modify, or disclose information belonging to other people without their permission, or the approval of the Managing Director or Director-owner.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening, or discriminatory. In the event that there is a genuine academic need to carry out an activity which might be interpreted as being in breach of the law (e.g. the deliberate viewing or accessing of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation;), cHRysos HR must be made aware of your plans in advance and prior permission to access must be obtained from the Managing Director or Director-owner.

8. Behaviour

When using cHRysos HR IT facilities and social networking platforms you must not:

- Cause offence, concern or annoyance to others including posting of inappropriate comments about learners/apprentices, members of staff, associates or the organisation. Genuine scholarly criticism and debate is acceptable.
- Use the IT facilities in a way that interferes with others' valid use of them.
- Undertake any illegal activity including downloading and storing information subject to copyright, except under a relevant licence, or with permission from the copyright owner.
- View, store or print pornographic images or video.
- Access or use sites or other media which are specifically designed to promote terrorism, or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under UK and international law.
- Send spam (unsolicited bulk email), forge addresses, or use cHRysos HR mailing lists other than for legitimate purposes related to cHRysos HR activities.
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth, storage or consumables.
- Undertake any activity which jeopardises the security, integrity, performance or reliability of electronic devices, computer equipment, software, data and other stored information.
- Deliberately or recklessly introduce malware or viruses.
- Attempt to disrupt or circumvent IT security measures.
- Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
- Download illegal copies of music, films, games, or other software, whether via file sharing services or other technologies. This facility is blocked, and permission will only be given where this relates to developing cHRysos HR services or key operational needs.

9. Safeguarding and Prevent Duty

Should you become aware of or suspect that any individual is using cHRysos HR IT facilities, social media platforms or other media to harass, sexually harass, bully, harm or exploit any individual or to attempt to radicalise any individual or in the course of their own involvement in extremism, radicalisation or terrorism this must be reported immediately through the cHRysos HR Safeguarding and Prevent Duty policy and procedures or Equality, Diversity, Bullying and Harassment Policy as appropriate.

If you are personally subjected to harassment, sexual harassment, bullying, harm or exploitation, or are approached through IT, social media or any other media in the course of your work or studies with cHRysos HR, and encouraged to become involved in radicalisation, extremism or terrorism this must be reported immediately through the cHRysos HR Safeguarding and Prevent Duty policy and procedures or Equality, Diversity, Bullying and Harassment Policy as appropriate.

10. Home working

All employees and associates must also refer to the working from home policy/guidance and associated terms and conditions of employment.

11. Monitoring

IT and internet access via company owned equipment, are provided for legitimate use in relation to studying or business.

The company therefore reserves the right to monitor use of the internet, to examine systems and review the data stored in those systems. Any such examination or monitoring will be carried out by staff authorised to do so by the Managing Director or Director-owner.

You must not attempt to monitor the use of the IT facilities without explicit authority to do so.

Where there is a requirement to access the account of another member of staff, permission must be gained from the Managing Director or Quality Lead (in their absence).

If the request for access is related to a HR investigation, this must be managed wholly by the member of the management team or third party undertaking the investigation, in collaboration with the Managing Director or Director-owner.

All data written, sent, or received through the company's computer systems, social media platforms or other media is part of official cHRysos HR records. The company can be legally compelled to show that information to law enforcement agencies or other parties and will comply with lawful requests to do so.

Users should always ensure that information sent or uploaded through cHRysos HR's IT systems and other media is accurate, appropriate, ethical, and legal.

12. Implementation and enforcement of this policy

This policy is issued by the Managing Director and Director-owner of cHRysos HR Solutions Ltd.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of the implementation of this policy.

If you believe this policy has been infringed, you should report the matter to the Managing Director – email: sheila@chrysos.org.uk.

Follow up action will be considered carefully. Genuinely accidental infringement will be treated with understanding, but any deliberate or wilfully negligent infringement of this policy is likely to result in one or more sanctions being applied.

13. Potential sanctions

Breach of this policy is a serious matter. Employees who do so will be subject to disciplinary action which may result in termination of employment.

Where an associate is found to be in breach of this policy, their contract for services may be terminated.

Learners found to be in breach of this policy may be asked to leave their programme of study. Where apprentices studying with cHRysos HR are found to be in breach of this policy, the matter will be reported to their employer and may result in their removal from the apprenticeship programme.

Employees, associates, learners, apprentices, and other users may be held personally liable for violating this policy.

Information about deliberate infringement or illegal activities may be passed to appropriate law enforcement agencies, and any other organisations whose requirements you may have breached.

cHRysos HR reserves the right to recover from you any costs incurred because of your infringement.

This policy will be reviewed annually to ensure it remains fit for purpose.

The third-party IT company has authorisation to access all equipment and software and are also bound by all the requirements of this policy and legal requirements.

This policy aligns with cHRysos HR's Data Protection Policy.

Author	Sheila Moore
Position	Managing Director
Last reviewed	February 2025
Date for next review	February 2026
Signature