The Stables Independent School

Acceptable Use of Technology Policy for Staff

This policy links directly to the listed Stables Policies	Safeguarding Promoting Positive Behaviour & Relationships Online Safety

This policy was reviewed and approved by the Proprietors in Autumn term 2023. It will be reviewed annually and approved by the Proprietors.

Computers and the Internet are available primarily to support the functions of the job role. In instances where an individual's use of a Company computer or the internet is deemed irresponsible or inappropriate, access to the Company network will be removed for a period of time while the matter is investigated. Be aware that Internet searches and online activities are logged.

Company provided mobile phones are primarily used to support the job role and provide effective operation of the company. You should use your Company provided mobile phone responsibly and not for personal/social communication or gaming.

The ethos at the Company should make it apparent that a range of activities are absolutely prohibited when IT equipment is used. These activities include:

1. Sending, receiving or displaying offensive/obscene messages or images
2. Using IT to in any way harass, insult, embarrass or attack others

3. Using IT to ‘hack’ into others’ personal files. E.g. email, company records or private user-area/profile

4. Obtaining/using accounts or passwords of others when making use of any form of IT

5. Using IT to copy material or otherwise violate laws of copyright

6. Using obscene or offensive language/images when communicating

7. The deliberate damage or corruption of computers, systems or network peripherals

IT GUIDELINES (STAFF)

1. Keep your password secure. Do not tell anyone what it is. Change it regularly. If you suspect your password has been obtained by somebody else, you must inform IT Support ASAP.

2. A secure network is provided to the benefit of all. Respect the safeguards in place and do not attempt to bypass filters or user permissions, this activity will be logged. In particular do not use VPN tunnels, Proxy Servers or non- Company Internet Services to access blocked material. If a legitimate website is blocked, please contact IT Support: Netmatters on 01493 603204.

3. If you are using a computer and you find something suspicious, unpleasant or offensive please inform the Headteacher immediately. Be aware that Internet searches are logged.

4. Never give out personal information (including photos/videos/email address) to anyone you do not know. Never share your password with anyone, including friends or family. Data security at the Company is a collective responsibility.

5. If you receive a request asking you for any personal information, especially via email – stop, think and if unsure report it to the headteacher. It is extremely rare for an official provider to require you to send personal information online. Banks, PayPal, HMRC etc will either call or post a formal letter to which it is recommended you call back on a standard number to validate.

6. Do not open attachments if you are unsure of their content. If you don’t know what an attachment might contain, and you were not expecting to receive it please contact us.

7. Save your work regularly and backup all of your important files to your allocated private network share, particularly any work you store locally to your own device(s). If you save work to external media, it is your responsibility to keep it safe and avoid loss. Any loss/theft must be reported ASAP. Cloud storage is now a viable alternative to USB drives.

8. Avoid wasting file server storage. Please delete any out of date, duplicated or unwanted files. The Company reserves the right to delete non-work-related material from the network drive if we are running low on space. We strongly advise your personal files to be stored on non-networked devices or personal cloud drives.

9. When using a Company device remember to close down and log off your session correctly. **Never leave a device logged in/unlocked when you are not present.**

10. Copying software and/or music/movie files is illegal. Please respect the rights of authors and do not copy from any source without official permission this includes the company network. Those who do are liable for prosecution.

11. Think before you print, save paper whenever possible. Print job log files are retained. Shred any paper documents that are no longer required.

Internet:

All staff have access to the internet at The Stables. The internet is monitored and there are blocks in place on accessing certain website (social media, gambling, pornography, dating websites). Staff will carry out cyber checks in planned ways and inform other appropriate staff of any planned ones so that checking for inappropriate content is not mistaken for intentionally attempting to access.
The internet is only to be used for work related matters during working hours of 8am-6pm.

Staff are permitted to use the internet outside of these times as long as this is used appropriately.

Staff should not download nor delete any programmes from the internet without consultation or direct instruction.

Information/pictures regarding a young person should never be put on the internet by staff.

General Data Protection Regulation

The GDPR establishes standards for the handling of personal data (data which identifies, or could be used to identify, a natural person). Principally the regulation is concerned that data is handled “lawfully, fairly and in a transparent manner” and protected “against unauthorised or unlawful processing and against accidental loss”. You have a duty to help protect personal data held and used by the Company and to use personal data only for the purposes intended and approved by the Company.

Staff should note that unauthorised disclosure and in particular any deliberate breach by a member of staff may be treated as a disciplinary matter and may be considered gross misconduct in some cases, serious breaches may lead to dismissal.

No set of guidelines can cover all possible situations, staff must use their own judgement to protect personal data and seek advice when unsure.

Along with the existing liabilities for illegal disclosure of data, there are two new criminal offences for which you may be held personally responsible by a court:

It is an offence to knowingly erase or alter personal data which is currently part of a request under a data subject's right to access.

It is an offence to re-identify data which has been treated with a technique to prevent identification of the data subject (i.e. to "de-anonymise" data which has been "anonymised").

Please follow the guidelines below to help ensure data is handled appropriately:

Personal information must not be disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

If you become aware of a breach of data protection you must report it immediately to The Data Protection Officer (DPO) via info@theprivacyworx.com.

If you receive a query about what data, we hold or a request about someone's rights with respect to personal data please contact The Data Protection Officer without delay.

Do not use data collected for one purpose for any other purpose without checking with the Data Protection Officer that this is lawful.

Do not retain personal data which you no longer require:

Check if there are any specific retention policies for your areas of responsibility.
Go through your outlook contact list at least once a year and delete contacts you no longer need.

Go through your emails at least once a year and delete those no longer relevant.

Go through your stored files at least once a year and delete those which you no longer need.
N.B. the company may have a legal obligation to retain certain records (contact The Data Protection Officer if you need further advice).
Do not share data with colleagues unless necessary and do not seek or accept access to data you do not need to complete your professional responsibilities. If in doubt, ask your supervisor or contact The Data Protection Officer for advice.

Do not accept personal data you do not need. If you are sent personal data which is unnecessary, irrelevant or inappropriate delete it immediately.

Do not transfer personal data from Company computers or networks to other networks, cloud storage or non-Company memory sticks, laptops, tablets or mobile telephones, unless specifically authorised in writing.

Email to addresses outside the "@thestablesschool.co.uk" domain should not include personal data beyond simple contact information (name, email, telephone, job title and place of work). If more extensive data needs to be provided, please use an encrypted

attachment (MS 365 encryption is adequate for low-risk data) or contact The Data Protection Officer about secure transfer options.

Do not include the password for an encrypted attachment in the same email and preferably use a different communication method to send the password (e.g. SMS). Emails sent from "@thestablesschool.co.uk" addresses to "@thestablesschool.co.uk" addresses are restricted to the secure environment and may include personal data. Do not include any personal information in the "Subject" field of email regardless of the recipient.

Make it a habit to use "Bcc" rather than "Cc", "Cc" should only be used where it is necessary for all recipients to see replies.

When using Distribution Lists to send emails to those outside the company, ensure that email addresses are not shared. Use the "Bcc" facility so that email addresses are not displayed.

If you wish to use your personal mobile phone for company email you must obtain permission from a Director/responsible person in advance. The Director will require you to ensure your mobile phone is PIN protected.

Do not leave paper copies of documents containing personal data unsecured, use locked file cabinets whenever possible and if you need to leave your office temporarily unattended whilst working with such documents you must close and lock the office door.

Social Media

'Social Media' is the collective term commonly given to websites and web applications that are used to discuss, debate and share information on - line. The most common types are: social networking, blogs, micro-blogging, content communities, wikis and forums, examples of which include, Facebook, X, LinkedIn, YouTube, Instagram, Snapchat and Wikipedia.

Employees are not to comment on their work on any external web pages. There must be no overt or covert mention of any Clover Childcare Services employees or any young people who attend, or have attended, the school.

Should employees become aware of negative or disparaging remarks about the company, its staff or its services, they should not respond but instead advise their Director who will determine if the comments merit disciplinary action.

Staff must ensure that their use of the internet, social media and e-mail does not compromise or breach the standards of professional conduct expected of them and are advised to use private settings and not to have open or public media social connections.

Making social connections (such as adding friends on Facebook, followers on Twitter, gaming) is not permitted at all between the young people and staff. This also extends to the young people's friends, family and other associates.

This is to maintain a good safeguarding culture and appropriate boundaries. Any deviations of this will result in action taken against the staff member. Staff should also

remain vigilant when accepting requests from unknown people in case this a young person attempting to infiltrate staff's social media. Staff are also obliged to inform management in any cases of young people attempting to make connections and this will be discussed sensitively and openly with the young people involved.

Social connections with young people who have left Clover Childcare Services is not advised or supported unless the member of staff has express permission from the social care team of the young person.

There are no contractual restrictions on social media connections with young people over the age of 18 years, unless that young person is still residing at Clover Childcare Services.