GDPR – Staff guidance on remote working

This policy and procedure applies to employees of St Dunstan's Trustee Limited on behalf of St Dunstan's Education Foundation & College Hire Limited.

Be Vigilant – No one in your household should have access to or see the personal data you are using

- Be aware of your surroundings and who may be able to view your screen/work.
- Do not write down your passwords on paper where they can be discovered.
- Use strong passwords to protect your work devices and make sure you use a password that no-one else in the household knows or can guess.

Remember your data protection training to help you to ensure that everything is kept safe whilst at home

- Protecting student and staff data must remain the highest priority. Data breaches can cause real and significant harm to individuals and the risk of data breaches become much higher when data is accessed remotely or on a portable device.

Using your electronic device (personal or loaned from the Foundation) to access the Foundation network

- Check that your device is fully up to date with anti-virus, firewall, malware and security updates.
- Ensure that work documents are saved on the Foundation network or your Foundation one drive account securely rather than on the desktop or in "my documents."
- Ensure your device has a password or (for tablets/phones) pin code. Passwords should be complex (a mixture of numbers, letters and capitals).

Ensure that if you are communicating remotely via video conferencing with your colleagues or students that:

- You use platforms which have been approved by the Foundation.
- Ensure that webcams are only activated when they need to be.
- Do not record unless authorised to do so by the Foundation (and the participants to the call also consent).
- Please ensure that you are appropriately dressed
- 'Blur' your background or ensure that it is appropriate (for example, a bedroom would not be considered an appropriate view)

Reviewed: Lent 2023
Next Review: Lent 2024

- Screen share facilities should not contain personal data where possible. Please share any relevant documents to attendees prior to the meeting for all to view
- Any safeguarding issues should be reported to the DSL immediately

E-mail communications between staff, students and parents:

- All communications must be sent from your Foundation e-mail address and **never** your personal account
- Do use iSAMs to communicate with parents and students in the first instance, particularly if you are communicating with several people at a time to deliver the same/similar message
- If you are using your Outlook account to communicate with several parents, it is extremely important that any other parents are blind copied (bcc) in rather than just copied (cc) into. It can be a significant data breach if this is not the case, as all parents will now have access to other parent's e-mail addresses.

Ensure not to give out your personal details, such as a mobile phone number and personal email address to pupils.

- Do not use personal email accounts or telephone numbers for Foundation use.
- If making calls, please utilise the new 3CX phone system (details have been e-mailed to all staff) this provides you with the facility to call from your Foundation phone extension number, with no charge to you personally and no sharing of your own personal number.

Lock your screen while you are away/not using your device

- Please be vigilant to lock screens when not in use for long periods or where you are stepping away from your device. In addition, devices should be shut down at the end of the day.

Ensure that Foundation IT equipment is kept in a secure place

- It is your responsibility to ensure that Foundation equipment is kept secure (for example in a locked draw). If a device becomes lost or stolen, please report this to the Foundation without delay and within 72 hours.

Do not use your own USB memory sticks and plug them into Foundation devices to take data from Foundation systems or to upload data or documents to Foundation systems

- This goes for memory sticks, pen drives, external hard drives. They should not be plugged into Foundation devices unless they are issued/approved by the Foundation IT team.
- Ensure that any memory stick, pen or external hard drive is encrypted or contain passwords and pin codes to access the information stored on them

Do not install or download any software onto a work device without the approval of the Foundation.

- Where approval is given, they should also be virus checked before they are downloaded onto the Foundation's systems.

Always be careful which websites you visit and which emails attachments you open.

- Be careful when opening attachments to emails - even if the message appears to be from someone you know. Email attachments infected with viruses are one of the most widely used methods for infecting PCs.
- Be vigilant against phishing attacks claiming financial rewards or encouraging charity donations. Phishing emails can look like they came from a real company or person you know and trust. The sole purpose of a phishing email scam is to trick you into going to a fake website that looks equally authentic and inputting personal information that would in turn provide the criminal with access to your accounts.
- Remember that text, music and other content on the internet are copyright works. You should not download or email such content to others unless certain that the owner of such works allows this.

Ensure you keep your own shared area and own email accounts organised.

- Do not keep emails or documents for longer than you need, and it is each individual's responsibility to ensure their accounts are organised appropriately. If necessary, check the Foundation's Retention Policy and Schedule and ensure that you are complying with it and not storing personal data longer than you are allowed to.

Paper records count too

- Paper documents taken from Foundation or printed off at home must be kept secure at home just as they would be at Foundation.
- At the end of the working day, or when you leave your workstation unoccupied, all paper documents containing personal information need to be securely locked away to avoid unauthorised access.
- You must ensure that documents are returned to secure storage at Foundation as appropriate or they are destroyed securely at home. (see Foundation's retention policy).
- Do not put confidential waste into the ordinary waste. Ensure that it is shredded first.

Do report any breaches of the above to the Chief Operating Officer and refer to our Acceptable Use policies.