Policy and Procedure Number:	C17	
Management Area:	Whole School	
Reviewer: Mike Bradshaw – Deputy Head		
Last Reviewed: October 2021		
Next Review: October 2022		
ACCEPTABLE USE OF IT, THE INTERNET AND ELECTRONIC COMMUNICATION - Staff		

FREDERICK
GENT
SCHOOL

CONTENTS

This policy should be read in conjunction with:
A08 Child Protection and Safeguarding
D08 Data Protection Policy
C23a TTCT Social Media Policy
D12 TTCTCode of Conduct

1. Introduction

The School's IT resources are essential to the effective delivery of educational provision. Computers and other networked facilities, including internet access, are available to staff and students within the school and should be used to promote educational learning. It is therefore vital that all staff, agents and contractors are aware of the School's policies and procedures relating to the use of IT resources.

2. Scope

2.1 This policy applies to all technology and communications equipment provided by TTCT.

2.2 This policy applies to all employees of The Two Counties Trust, agency staff, volunteers, placements, Governors and those working on behalf of The Trust.

3 Safe Working Practice

3.1 Staff should make careful, considerate use of the school's IT resources, report faults and work in a way that minimises any risk to the system.

3.2 Staff are responsible for maintaining the security of computers and networks by only using their own logon details and not allowing other staff or pupils to use their personal passwords. Staff should ensure that they either lock or log-out from all unattended machines.

3.3 Staff should ensure that when using work equipment at home, other family members do not use the equipment for their personal use. Staff are responsible for all the content (software and data) on any equipment allocated to them.

3.4 Staff should not install any unlicensed software on machines allocated to them.

3.5 Staff must follow the school's safeguarding protocols to protect students from harmful or inappropriate material accessible via the Internet or through other electronic means. For further guidance, please refer to the Safeguarding policy.

3.6 Staff must ensure that they understand and uphold the following when using the school access to the Internet:

- Personal use of the Internet is limited to employees' own time.
- Use of the Internet via TTCT or school equipment should exclude use for trading or personal business purposes.
- Use of the Internet to buy goods or services will not render the TTCT or school liable for default of payment or for the security of any personal information disclosed. Staff are advised not to use the school's computer system for making payments.

- Personal goods must **not** be delivered to the School.

3.7 Staff have a responsibility to ensure the appropriateness of sites visited on the Internet. As such, staff must not deliberately view a site or copy/ circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material, the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains images, cartoons or jokes that will cause offence
- that constitutes bullying

3.8 In any case where an Internet site that contains unacceptable material is visited or accessed, staff should inform the headteacher as soon as possible. The headteacher will use their professional judgement whether to report the matter further. In this situation the staff member should ensure a short written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

3.9 Staff must ensure that in using the internet, they do not infringe any copyright laws. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all down loaded material must be for curricular or research purposes and must not be passed to third parties.

3.10 Staff have a duty to uphold the reputation of the school and TTCT when using any form of IT. Staff should refer to Section 20 of The Two Counties Trust Code of Conduct **(Policy Number D12)** for further details.

4. Social Media

4.1 All staff should be expected to follow the guidance contained in The Two Counties Trust Social Media policy **(Policy Number C23a).**

4.2 Frederick Gent School's social media platforms are maintained by the Headteacher's PA. All requests should be directed to the Headteacher's PA.

4.3 Staff are not to use any other social media platform for work purposes.

5. Relationships between employees, the public, parents and students.

5.1 In all matters regarding the use of IT and Internet services and relationships between stakeholders, all staff should follow the expectations set out in Section 19 of The Two Counties Trust Code of Conduct **(Policy Number D12).**

6. Use of personal equipment

6.1 Only authorised school technology may be used to record children's activities. On trips, staff and volunteers should only use school devices for the purpose of taking photographs/videos. In a school, visitors accompanied by staff may be granted permission to use authorised devices for the purpose of recording work.

6.2 The school permits staff to use personal equipment such as mobile phones, tablets and personal computers to access the school's systems and emails where possible. In using such devices, staff must ensure that devices are equipped with a suitable level of encryption to ensure that information cannot be accessed by anyone other than the member of staff.

6.3 Staff are not permitted to use their own mobile phones and personal devices for contacting children.

6.4 Personal devices must not be used to take photos or videos of pupils and will only use school designated devices may be used for this purpose. If anyone sees someone using a personal device with a camera to take images, this should be reported immediately to the DSL or Deputy DSL.

6.5 Staff should not use personal mobile phones and other electronic devices for personal reasons whilst they are responsible for children in teaching situations and in the playground. Staff may access their personal devices whilst off duty but not in designated areas used by children.

6.6 On off site visits, adults should ensure that they have access to a school mobile phone and this is switched on. These should only be used if there is an emergency or where there is need to contact school or parents. Where staff members are required to use a mobile phone for school duties, for instance in the case of off-site activities, phone numbers will be recorded on the school risk assessment forms.

6.7 If a member of staff needs to make an emergency call during teaching time, they must ensure the class is supervised and make or take the call in an appropriate area not designated for children. Where possible a LM should be made aware of the need to call.

6.8 Parents/Carers are permitted to use their own devices to take photos and videos at school event. They are not permitted to upload these to social media sites if they contain images of children, other than their own. Parents/Carers must be reminded of this before performances.

6.9 Pupils will be provided with appropriate school devices to use in specific learning activities under the supervision of staff. The Headteacher reserves the right to check image content belonging to staff, parents, visitors or volunteers mobile phone or electronic devices, should there be cause for concern over the appropriate use of it. If inappropriate material be found, Child Protection procedures will be initiated.

7. Internet and Email

7.1 All employees are granted limited access to these facilities. Where use is personal, i.e. not in conjunction with an identified educational need or official school business, it should only take place during undirected time (i.e. lunchtimes, unpaid break, before and after your shift starts). In other words, you should not use the facilities for personal use when you should be carrying out school work.

Infringement of this policy by employees may be regarded as a disciplinary offence and, in serious cases, may result in dismissal. Improper use of the Internet or Email could bring the school into disrepute and may lead to legal claims against the individual and the school.

Improper statements in email can give rise to personal liability and liability for the school and may constitute a serious disciplinary matter. Emails that embarrass, misrepresent or convey an unjust, or unfavourable, impression of the school or its business affairs, employees, suppliers and their families are not permitted.

7.2 Use of e-mail and the Internet, which brings Frederick Gent School into disrepute, may result in disciplinary action.

7.3 Any personal or potentially personal information sent via e-mail and the Internet is covered by the Data Protection Act 2018. The Act requires all employees to take special care when handling personal information.

7.4 Emails between staff containing any personal information should have the word 'internal' inserted into the subject box to prevent the email from being forwarded or sent outside of the school system.

7.5 For external emails, no personal information should be included in the body of the email. Staff should use a password protected, attached document which must be sent separately from the password. Passwords must be sent no sooner than 5 minutes after the original email.

7.6 While personal use of the Internet and email is permitted during lunch breaks and out of working hours, staff should be aware that the facilities are provided by the school and any activity received/sent through the school's network, personal or otherwise, is recorded and will be monitored.

7.7 Staff should not engage in 'recreational' chatting during working time, on email or through instant messaging. The school's facilities must never be used for the passing of inappropriate personal information of any kind.

7.8 The school's default email settings should not be altered at any stage (for example, the footer, disclaimer, autosignature etc.)

7.9 Employees should take particular care that they have typed/selected the correct email address so that the information is not sent to an inappropriate person by mistake (e.g. students).

When email is used to communicate with students, parents or carers as part of a professional role, a school email address should always be used. The style and format of any such communication should be formal. Staff should always blind copy (BCC) a line manager into any contact with a pupil or parent as a further safeguard.

7.10 Extreme care must be taken when using the school's email facilities to transmit information. Confidential or sensitive information should not be sent via the Internet or email unless the data is protected. Staff should remember that when a Subject Access Request or Freedom of Information request is submitted, relevant email communications will be included in the material to be provided.

7.11 Employees must not use e-mail in any way that is insulting or offensive.

Employees must not deliberately view, copy or circulate any material that:

- could constitute bullying
- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcome propositions
- contains images, cartoons or jokes that will cause offence

8. Monitoring of email

8.1 The school reserves the right to make appropriate arrangements to monitor, log record and access all communications at any time without notice. Initially this is done via an electronic system, however if this was triggered by an employee's actions, this would be reported to the Headteacher. Where there was good cause, this situation would be more closely monitored by the management of IT services, but only if explicitly requested by the Headteacher. The Headteacher will record the reason for the monitoring. Whenever an employee's emails have been accessed/monitored, they will be notified and given the reasons. Other than this employees should be assured that no-one is allowed to read/access their emails.

The following details are recorded by the system in respect of every email message:

- name of the person sending the email,
- the email addresses of all recipients and copy recipients,
- the size and name of any file attachments,
- the date and time sent,
- a copy of the email,
- a copy of file attachments.

8.2 The school may produce monitoring information, which summarises email usage and may lead to further enquiries being undertaken.

Monitoring information will be kept in line with TTCT data retention schedule.

9. Monitoring Internet Access

9.1 Frederick Gent School records the details of all Internet traffic. This is to protect The Two Counties Trust and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

The logs record:

- the network identifier (username) of the user,
- address of the Internet site being accessed,
- where access was attempted and blocked by the system,
- the Web page visited and its content,
- the name of any file accessed and/or downloaded,
- the identity of the computer on the network and the date and time.

All monitoring information will be kept in line with TTCT data retention schedule.

Laptops issued to staff

10.1 The laptop remains the property of the School and is provided to users on a loaned basis. The laptop provided must not be used by any person(s) other than the authorised user to whom it has been allocated and the property identification tag attached to each laptop should not be removed for any reason.

10.2 School laptops have a predetermined list of software installed on the hard drive. No addition or deletion of any software or hardware is permitted without the express permission of the the Headteacher. To ensure that security patches and virus definitions are up to date staff should connect the laptop to the School network on a regular basis.

10.3 All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, the laptop should never be left in a vehicle overnight or other unsecured, vulnerable situation. In addition, appropriate insurance should be in place to

cover these eventualities. Any loss or damage to School IT equipment should be immediately reported to the Headteacher or Schools IT manager.

10.4 When a contract of employment at the school ends, the employee must return all computer equipment and software to the school in full working condition immediately on the last working day. The user account and all personal work stored on the laptop will then be securely deleted.

10.5 If software/hardware problems arise, the laptop may need to be restored to its original settings. Work files may be lost during the restoration process, therefore it is the responsibility of all users to ensure that backups of all files are regularly made to an external device, such as the School's networked server or via cloud based storage such as Microsoft Office.

10.6 Where there is evidence that the laptop has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any School laptop whilst on loan.

11. Working with Display Screen Equipment (DSE)

11.1 All staff should refer to the TTCT Working with Display Screen Equipment policy **(Policy Number C25c)** for further guidance on the usage and monitoring of usage of display screens.

11.2 LM will conduct a DSE review each year for all based staff. The findings will be shaped by the DP for Health and Safety.

12. Use of other School IT Equipment

12.1 Users who borrow equipment from the School must sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the Headteacher or the IT Services Manager by email in the first instance, and any theft or criminal damage should also be reported to the Police.

13. Software

13.1 Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the School. Under no circumstances should any user possess unlicensed software on School premises or use unlicensed software on School IT equipment (including portable equipment).

14 Network Access, Passwords and Data Security

14.1 Users must only access information held on the School's computer systems if properly authorised to do so and the information is needed to carry out their

work. Under no circumstances should personal or other confidential information held on the School network or IT equipment be disclosed to unauthorised persons. Any accidental access of information for which you are not entitled to view, report this immediately to the Deputy Headteacher.

14.2 Staff should neither access personal or sensitive information in the presence of students, nor should they display any information held about other students on a whiteboard or similar. Staff using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer. In other areas computers must not be left logged on when unattended (this includes in offices and at home). Staff must never allow anyone else, especially students, to use a workstation which they have logged on to. When printing sensitive data, staff should always beware that the correct printer has been selected and that the information is collected immediately so that there is no breach of data security.

14.3 Staff passwords must be at least eleven characters in length, containing at least two of the following: one capital letter, one symbol or one number. Whilst the user account is active the password must be changed on a regular basis, at least termly. System and administration level passwords should also be changed, at least on a termly basis.

All passwords are to be treated as sensitive, confidential information. Therefore, staff must not:

- write down passwords or store them on-line.
- use School user account passwords for other types of access (e.g., personal ISP accounts, Internet banking, etc.).
- share passwords with anyone, including line managers, colleagues, administrative assistants, secretaries, or IT Technicians.
- reveal a password over the phone or in an e-mail message or other correspondence.
- talk about a password in front of others including family members.
- hint at the format of a password (e.g., "my family name").
- reveal a password on questionnaires or security forms.
- insert passwords into e-mail messages or other forms of electronic communication.

14.4 If an account or password is suspected to have been compromised, the incident must be reported immediately to the Head Teacher or IT Services Manager so that the account password can be changed.

15. Disciplinary and Related Action

15.1 Suspected misuse of the School's computer systems by a member of staff will be considered by the Head Teacher. Failure to follow the IT Acceptable Use Policy could result in disciplinary action being taken and include a warning,

suspension, dismissal from the School and in the case of illegal activities referral to the Police.