TOWNLEY

EST 1937

GRAMMAR SCHOOL

ACCEPTABLE USE OF ELECTRONIC INFORMATION & COMMUNICATIONS SYSTEMS POLICY

1. Introduction

Townley Grammar School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. In order to ensure the safety of both staff, trustees and students, it is important that all staff members and trustees follow the guidelines detailed below.

This policy outlines the standards that Townley Grammar School requires all users of these systems to observe, the circumstances in which Townley Grammar School will monitor use of these systems and the action Townley Grammar School will take in respect of any breaches of these standards.

The use by staff and monitoring by Townley Grammar School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to Townley Grammar School's Data Protection Policy for further information. Townley Grammar School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

Townley Grammar School has the right to monitor all aspects of its systems, including data which is stored under Townley Grammar School's computer systems in compliance with the UK GDPR.

This policy aims to:

• Promote the professional, ethical, lawful and productive use of Townley Grammar School's ICT systems and infrastructure. Including use (or misuse) of computer equipment, e-mail, internet connection, telephones, Mobile phones, Laptops, Chromebooks, iPads (and other mobile device tablets) and voicemail, but it applies equally to the use of printers, copiers, scanners, and the like.
• Define and identify unacceptable use of Townley Grammar School's ICT systems and external systems.
• Educate users about their data security responsibilities.
• Describe why monitoring of the ICT systems may take place.
• Define and identify unacceptable use of social networking sites and school devices.
• Specify the consequences of non-compliance.

This policy applies to staff members and trustees, and all users of Townley Grammar School's ICT systems are expected to read and understand this policy. Breach of this policy may result in disciplinary action.

2. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright

- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorization
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

3. Equipment Security and Passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and staff are required to select a password that cannot be easily broken and which contains at least 8 characters including numbers and letters. All passwords should be considered complex.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Team who will liaise with the IT Services Team as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under Townley Grammar School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to Townley Grammar School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and/or IT Services Team may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, Townley Grammar School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information. Logging off prevents another member of staff or a pupil accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of our IT Services Team.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed. Townley Grammar School reserves the right to require employees to hand over all school data held in computer useable format.

Members of staff who have been issued with a laptop, Chromebook, iPad (or other mobile device tablet), Smart Phone or any other device (i.e., USB stick) must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the device is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g., ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers. If staff take devices off-site, they should follow the Home Working Policy.

4. Systems Use and Data Security

Members of staff should not delete, destroy or modify any of Townley Grammar School's existing systems, programs, information or data which could have the effect of harming or exposing to risk of harm Townley Grammar School, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the IT Services Team who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

All members of staff need to inform the Data Manager before sharing any data with any third parties so Townley Grammar School can carry out a Data Protection Impact Assessment (DPIA).

Where consent is given, all files and data should always be virus checked before they are downloaded onto Townley Grammar School's systems. If in doubt, the employee should seek advice from the IT Services Team or a member of the Senior Leadership Team.

No device or equipment should be attached to our systems without the prior approval of the IT Services Team or Senior Leadership Team. This includes but is not limited to, any Smart Phone or telephone, iPad, laptop (or other mobile device tablet), USB device, i-pod, digital camera, infra red connection device or any other device.

Townley Grammar School monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). The IT Services Team should be informed immediately if a suspected virus is received. Townley Grammar School reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. Townley Grammar School also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of Townley Grammar School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of Townley Grammar School's Systems and guidance under "E-mail etiquette and content" below.

5. E-mail Etiquette and Content

E-mail is a vital business tool but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

Townley Grammar School's e-mail facility is intended to promote effective communication within the business on matters relating to Townley Grammar School's business activities and access to Townley Grammar School's e-mail facility is provided for work purposes only.

Staff are prohibited from using Townley Grammar School's email facility for personal emails at any time. Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff should always consider if e-mail is the appropriate medium for a particular communication. Townley Grammar School encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with Townley Grammar School's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the e-mail to be read out in public or subjected to scrutiny then it should not be sent. Hard copies of e-mails should be retained on the appropriate file.

All members of staff should remember that e-mails can be the subject of legal action for example, in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and Townley Grammar School. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of Townley Grammar School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. They may also be disclosed as part of dealing with subject access requests when they arise. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader or themselves, if it found its way into the public domain. Townley Grammar School standard disclaimer should always be used on every e-mail.

Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied or are offended by material sent to you by a colleague via e-mail, you should inform HR who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under Townley Grammar School's formal grievance procedure. (Further information is contained in Townley Grammar School's Equality, Diversity and Inclusion Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

6. General Guidance

Staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside Townley Grammar School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals;
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail, the internet or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature;

Townley Grammar School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The Data Manager should be informed as soon as reasonably practicable.

7. Use of the Internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to Townley Grammar School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if for example, the material is pornographic in nature.

Staff must not access any web page or any files from Townley Grammar School's system (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms,

could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within Townley Grammar School (whether intending to view the page or not) might be offended by the contents of a page or if the fact that Townley Grammar School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time. Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

8. Personal Use of School Systems

Staff are prohibited from personal use of Townley Grammar School's systems.

Staff should be aware that any personal use of the systems may also be monitored (see below) and where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Excessive or inappropriate personal use of Townley Grammar School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Townley Grammar School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

9. Inappropriate Use of Equipment and Systems

Access is granted to the web, telephones and to other electronic systems for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with Townley Grammar School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- Transmitting a false and/or defamatory statement about any person or organisation;
- Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
- Transmitting confidential information about Townley Grammar School and any of its staff, students or associated third parties;
- Transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for Townley Grammar School);

- Downloading or disseminating material in breach of copyright;
- Copying, downloading, storing or running any software without the express prior authorisation of the IT Services Team.
- Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- Forwarding electronic chain letters and other materials;
- Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found Townley Grammar School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

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

10. Digital Cameras

Townley Grammar School encourages the use of digital cameras and video equipment; however, staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to Townley Grammar School network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted, unless it is a school phone.

11. File Storage

Staff members have their own personal area on the network, as well as access to shared network drives and Google Drive. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas.

Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data has to be transferred it must be saved on an encrypted, password protected, storage device
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

12. Mobile Phones

Mobile phones are permitted in school by staff, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. Townley Grammar School provides Trip phones for this purpose.
- All phone contact with parents regarding school issues will be through Townley Grammar School's phones. Personal mobile numbers should not be given to parents at Townley Grammar School.

13. Personal Social Media Accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

14. Remote Access

We allow staff to access the school's ICT facilities and materials remotely via LGFL. You can request access to this through IT Services.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the headteacher may require against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.