The Dunstan Catholic Educational Trust

IT Acceptable User Policy

Date: September 2024

Review Date: September 2025

This policy applies to all Schools within the DCET

1 **Introduction:**

ICT is provided to support and improve the teaching and learning in our Trust as well as ensuring the smooth operation of our administrative and financial systems.

This policy sets out the requirements with which you must comply when using the Trust's IT and when otherwise using IT in connection with your job including:

- The Trust's email and internet services.
- Telephones and faxes;
- the use of mobile technology on Trust premises or otherwise in the course of your employment (including 3G / 4G / 5G, Bluetooth and other wireless technologies) whether using a School, Trust or a personal device; and
- any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the Trust.
- This policy also applies to your use of IT off Trust premises if the use involves Personal Information of any member of the Trust community or where the culture or reputation of the Trust or any of its Schools are put at risk.
- The policy also provides advice and guidance to our employees on the safe use of social media which should be read in conjunction with our social media policy.

Failure to comply: Failure to comply will constitute a disciplinary offence and will be dealt with under the Trust's Disciplinary Procedure.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may itself result in disciplinary action.

Property: You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to the School Business/Office Manager. You should not use the Trust's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

Viruses and other malicious code: You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not introduce use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails which have not first been checked by the Trust for viruses.

Passwords: Passwords should be long, for example you could use a song

lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else. In addition:

- Your password should be difficult to guess, for example you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.
- You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.
- Passwords (and any other security credential you are issued with such as a key fob) must be kept secure and confidential and must not be shared with, or given to, anyone else.
- Passwords should not be written down.

Leaving workstations: If you leave your workstation for any period of time you should take appropriate action and, in particular, you should log off and/ or set your screen saver with an appropriate password.

Concerns: You have a duty to report any concerns about the use of IT at the Trust to [• the Head]. For example, if you have a concern about IT security or pupils accessing inappropriate material.

Other policies: This policy should be read alongside the following:

Code of Conduct;

Trust-wide Data Protection Policies; and

Acceptable use policy for pupils.

Internet

Downloading: Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

Personal use: The Trust permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the Trust discovers that excessive periods of time have been spent on the internet provided by the Trust or it has been used for inappropriate purposes (as described in section below) either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Headteacher

Unsuitable material: Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the Trust believes is unsuitable, at any time, is strictly prohibited and constitutes gross misconduct. Internet access may be withdrawn without notice at the discretion of the Head whilst allegations of unsuitable use are investigated by the Trust.

Location services: The use of location services represents a risk to the personal safety of those within the Trust community, the Trust's security and its reputation. The use of any website or application, whether on a Trust or personal device, with the capability of publicly identifying the user's location while on Trust premises or otherwise in the course of employment is strictly prohibited at all times.

Contracts: You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the Trust or any of its Schools, without specific permission from the Headteacher. This applies both to "free" and paid for contracts, subscriptions and Apps.

Retention periods: The Trust keeps a record of staff browsing histories for a period of 6 months.

Email

Personal use: The Trust permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled 'personal' in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The Trust may monitor your use of the email system, please see paragraphs 26 to 30 below, and staff should advise those they communicate with that such emails may be monitored. If the Trust discovers that you have breached these requirements, disciplinary action may be taken.

Status: Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

Inappropriate use: Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

Legal proceedings: You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may

exist on a back-up system or other storage area.

Jokes: Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the Trust's IT system to suffer delays and / or damage or could cause offence.

Contracts: Contractual commitments via an email correspondence are not allowed without prior authorisation of the Headteacher.

Disclaimer: All correspondence by email should contain the Trust's disclaimer.

Data protection disclosures: Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). **Staff must be aware that anything they put in an email is potentially disclosable**.

Monitoring

The Trust regularly monitors and accesses its IT system for purposes connected with the operation of the Trust. The Trust IT system includes any hardware, software, email account, computer, device or telephone provided by the Trust or used for Trust business. The Trust may also monitor staff use of the Trust telephone system and voicemail messages. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).

The purposes of such monitoring and accessing include:
to help the Trust with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

to check staff compliance with the Trust's policies and procedures and to help the Trust fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

Monitoring may be carried out on a random basis and it may be carried out in response to a specific incident or concern.

The Trust may also use software which automatically monitors the Trust IT system (for example, it would raise an alert if a member of Staff visited a blocked website or sent an email containing an inappropriate word or phrase.

The monitoring may be carried out by senior leaders in conjunction our IT providers. If anything of concern is revealed as a result of such monitoring then this information may be shared with appropriate senior leaders and

this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police. Social networking and use of the chatrooms, community forums and messaging using any device

The internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, Twitter, Instagram, LinkedIn, blogs and wikis. Use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during off duty time.

(a) You should exercise caution when using social networks. You must not communicate with pupils over social network sites. You must block unwanted communications from pupils. You are personally responsible for what you communicate on social media.

(b) You must never knowingly communicate with pupils in these forums or via personal email account or personal mobile phones.

(c) You must not interact with any ex-pupil of the Trust who is under 18 on such sites.

(d) Communication with pupils should only be conducted through our usual approved channels. This communication should only ever be related to our business.

(e) You must not post disparaging or defamatory statements about:
   (i) our Trust;
   (ii) our pupils, parents or carers;
   (iii) our governors or employees;
   (iv) other affiliates and stakeholders.

(f) You should avoid communications that might be misconstrued in a way that could damage our reputation, even indirectly.

(g) You should make it clear in social media postings that you are speaking on your own behalf. Write in the first person and use a personal email address when communicating via social media.

(h) If you disclose that you work at the Trust], you must also state that your views do not represent those of the Trust. You should also ensure that your profile and any content you post are consistent with the professional image you present to pupils and colleagues. Take care to avoid posting comments about Trust related topics even if you make it clear that the views do not represent the views of the Trust; your comments could still damage our reputation.

(i) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you have discussed it with your line manager.

Prohibited Acts

The following acts are prohibited in relation to the use of our IT systems and will not be tolerated:

(j) Violating copyright laws
(k) Attempting to harm minors in any way
(l) Creating, viewing, accessing, uploading, posting, messaging, downloading or otherwise transmitting pornographic, discriminatory, offensive, or criminal material
(m) Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity
(n) Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service
(o) Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)
(p) Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party
(q) Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.
(r) "Stalking" or otherwise harassing any user or employee
(s) Collection or storage of personal data about other users
(t) Attempting to access, or accessing restricted areas of the network, or to any password protected information, unless authorised by the Headteacher or as a recognised part of your role.