The Dean Close Foundation

Acceptable Use of Information Technology (IT) for Staff Policy (W056)

Registered Charity No: 1086829

Date of Issue: September 2026
Review Date: September 2027
Owner: Foundation Lead for Safeguarding and Health

DEAN CLOSE FOUNDATION

Acceptable Use of IT Policy for Staff

1. This policy applies to all Dean Close Foundation employees (including peripatetic teachers and coaches), volunteers and any adult accessing Foundation IT facilities. It describes what the Foundation considers acceptable use of School IT systems and data.

2. For the protection of the Dean Close Foundation, young people, staff, and volunteers it is necessary to set out guidelines for all online activity. Staff and volunteers should read this policy carefully, and comply with all aspects, in conjunction with other Dean Close Foundation policies.

3. The use of electronic communication and information retrieval is no more than another medium. The same behavioural and professional standards are expected of all Dean Close Foundation staff and volunteers as are the case with written communications, the telephone and face to face meetings.

4. Dean Close Foundation employees and volunteers must also comply with appropriate government legislation including:

    a. Online Safety Act 2023
    b. Computer Misuse Act 1990
    c. Data Protection Act 2018 (UK GDPR)
    d. Keeping Children Safe in Education 2026 or later
    e. Working Together to Safeguard Children 2026

5. By using Foundation IT systems all staff and volunteers are agreeing to the terms of this policy. Failure to adhere to this policy, and any related policies, may be regarded as a disciplinary matter and be treated as such.

6. As a general principle, internet access is provided to Dean Close Foundation employees and volunteers to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the Foundation considers to be acceptable uses of the internet:

    a. To provide communication within the organisation via email or the organisation website
    b. To provide communication with parents, guardians, and pupils, primarily via email on school matters
    c. To provide communication with other organisations for educational purposes
    d. To distribute electronic copies of School or Foundation publications
    e. To distribute details regarding organisation meetings
    f. To provide electronic methods of communication
    g. Any other use that directly supports work related functions
    h. To provide reasonable personal access during the working day

7. It is recognised by the Foundation that residential staff require greater access to the internet and Foundation equipment for personal use outside normal school hours, but the terms of this policy are applicable at all times.

8. Staff should always behave professionally when using Foundation equipment and/or Foundation internet provision. The following principles should be considered in all online activity:

    a. The Foundation cannot guarantee the confidentiality of content created, shared, and exchanged via school systems. Staff must ensure that online communications, and any content shared online, are respectful of others and composed in a professional manner
    b. The privacy of others must always be considered and respected. Photos, videos, contact details or other members of the school community cannot be shared without appropriate consent
    c. Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

9. The following uses will be regarded as not acceptable:

    a. Use for racial, sexual, homophobic or other harassment
    b. Use of non-educational games during working hours
    c. To solicit personal information with the intent of using such information to cause harm
    d. Entering into a commitment on behalf of the Foundation or School (unless explicit permission has been given)
    e. Visiting internet sites or accessing material that contains obscene, hateful, pornographic or otherwise illegal or unacceptable material
    f. Using Foundation IT provision to perpetrate any form of fraud, or copyright infringement, or music piracy
    g. Any actions that compromise the security of the network such as attempting to bypass the filtering system or the use of an unauthorised VPN
    h. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
    i. Hacking into unauthorised areas
    j. Publishing defamatory and/or knowingly false material about the Foundation or School, colleagues and/or pupils on social networking sites, 'blogs', social media, or any other online publishing format
    k. Revealing confidential information about the Foundation or School in a personal online posting, upload, or transmission - including financial information and information relating to pupils, staff and/or internal discussions
    l. Use of personal email to communicate with or about any Dean Close pupils
    m. Undertaking deliberate activities that waste staff effort or networked resources
    n. Introducing any form of malicious software into the Foundation or School network

o. To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet
p. Use of any peer to peer or Bit torrent systems
q. Use for private business purposes or personal matters that interfere with normal School duties

10. The following general principles should be adopted when using the internet at School or on Foundation or School business:

    a. Be polite. Abusive or offensive language should not be used
    b. Always use appropriate language. Any communication via a Foundation network could be seen as being sent on behalf of the Foundation and the network is not private
    c. Emails should be answered promptly (preferably within 36 hours) but hasty responses to challenging emails should be avoided
    d. Foundation staff must only access school IT systems using their own username and password. These should not be shared, and pupils must not be given network passwords not generally available to them
    e. The Foundation monitors the use of all IT systems and can view content accessed or sent via its IT systems.

11. It is the responsibility of each user of the Foundation IT system to protect their user account details and observe the following:

    a. Usernames or passwords must not be shared with anyone else, written down or stored electronically except in an encrypted or password protected form
    b. It is a requirement to choose a new password periodically. Follow the guidelines provided to choose a secure one
    c. Avoid using the same password for Foundation and other devices.

12. The Foundation maintains the right to monitor the volume of internet traffic generated, together with the internet sites visited by members of staff, to investigate excessive or inappropriate use and to block websites deemed inappropriate.

13. Staff internet usage is managed by the same Firewall system as pupils with more permissible categories. The IT department is able to unblock websites and change firewall rules. Requests for such should have an educational justification.

14. The provision of Foundation email accounts, Wi-Fi and internet access is for official Foundation business, administration and education. Staff should keep their personal, family, and social lives separate from the Foundation IT systems and limit as far as possible any personal use of these accounts

15. When using the School email system remember:

    a. Whenever an email is sent, it should be from an official Dean Close email address which includes your name, job title and the Dean Close name and logo
    b. Every user is responsible for all mail originating from their user ID (e-mail address)

c. Forgery or attempted forgery of electronic mail is prohibited
d. Attempts to read, delete, copy or modify the email of other users are prohibited
e. Messages or attachments form unknown senders should not be opened to minimise the risk of viruses entering the network. All emails received on Foundation networks from outside sources carry a warning banner which should be considered before an email is opened
f. The sending of junk mail, spam and chain letters are prohibited
g. If an email is received from outside the Foundation that you consider to be offensive or harassing, report it to the IT helpdesk
h. All staff need to be aware that, in the event of the Foundation being involved in legal proceedings, such as a Subject Access Request (SAR), any relevant emails (including internal email) may have to be disclosed, as well as social media posts on Foundation devices and written documents
i. When accessing School emails on personal devices care must be taken to prevent unauthorised access to confidential information.

16. The Foundation reserves the right to access, review, copy, delete, disclose, or use staff school email files at any time and without notice. Staff emails can be monitored in line with privacy legislation, without prior notification, if it is deemed necessary for the purpose of ensuring this policy, or related policies are being adhered to.

17. When a member of staff or volunteer leaves the Foundation, their accounts in systems provided by the school will be suspended and the files and emails they have produced will be retained for a period of three years, in line with the Foundation's data retention schedule and to meet safeguarding, legal and insurance obligations.

18. If staff use their personal devices for Foundation business and/or on a Foundation network, this policy must be followed, and due regard given to data protection, privacy, and safeguarding.

19. Staff need to be aware that the use of the Foundation networks is monitored, and reports made to the Designated Safeguarding Lead (DSL) of any use that is not permitted by the Foundation Firewall or is of a safeguarding concern. Weekly reports on staff usage of the Foundation networks are produced and viewed by the relevant DSL.

Social Media

20. A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chatrooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Snapchat, Instagram, LinkedIn, YouTube, TikTok, Twitter (X) and Wikipedia.

21. This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using Foundation IT facilities and equipment or equipment belonging to members of staff or any other IT equipment.

22. Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether Foundation equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with the Foundation investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

23. 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 result in disciplinary action.

24. Whilst on social media, staff must:

    a. Ensure that wherever possible their privacy settings are set so that pupils cannot access information relating to their personal lives
    b. Obtain the prior written approval of the Head, to the wording of any personal profile which you intend to create where the School is named or mentioned on a social networking site
    c. Seek approval from the Head before they speak about or make any comments on behalf of the Foundation or School on the internet or through any social networking site
    d. Report immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the Foundation or School or raises any safeguarding concerns about pupils within the Foundation
    e. Immediately remove any internet postings which are deemed by the Foundation to constitute a breach of this or any other Foundation policy
    f. Consider whether a particular post puts their effectiveness as a teacher or Foundation employee at risk. Remember that colleagues, prospective employers, parents, and children may see your online information
    g. Protect themselves and other employees of the Foundation from identity theft

25. Whilst on social media, staff must not:

    a. Speak for Dean Close unless they have express permission to do so, this covers all comments relating to an individual school or the Foundation, staff, parents, and pupils
    b. If posts can be linked to the Dean Close Foundation, staff are expected to act appropriately and in line with the Staff Code of Conduct.
    c. Provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the Foundation and create legal liability for both the author of the reference and the Foundation
    d. Post or publish on the internet or on any social networking site, any reference to the Foundation or School, colleagues, parents or pupils without permission
    e. Use commentary deemed to be defamatory, obscene, proprietary, or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations

f. Discuss pupils or colleagues or criticise the Foundation or School or staff
g. Post images that include pupils
h. Harass or bully other members of staff
i. Attempt to communicate with pupils on any personal social network sites
j. Initiate friendships with pupils on any personal social network sites. Staff must decline any pupil-initiated friend requests
k. Dean Close Foundation policy is that staff are not allowed to be 'friends' or 'follow' current pupils in any part of the Foundation. Online friendships with Old Decanians is permissible but staff must ensure that settings are on private and only they and their friends can see them. If in doubt, please seek the advice of the IT department

Instant messaging

26. Instant messaging services such as WhatsApp are effective communication tools for staff and older pupils. These services offer end-to-end encryption between users; however, staff should be aware that messages sent or received on a Foundation device or account may still be accessed, reviewed and disclosed by the Foundation as set out below.

27. Foundation staff are welcome to set up instant messaging groups to aid rapid communication on Foundation matters. However, the following points must be born in mind:

    a. The same rules about the content of messages stated above apply to instant messaging
    b. Staff can be in the same instant messaging group as pupils but only for very specific reasons such as on a school trip, sports team, or house group. The line manager of the member of staff should be aware of the group and any concerns about use should be reported to a member of SLT immediately
    c. WhatsApp requires a minimum age of 13 for users. Staff should not use this platform to communicate with younger pupils but use a SMS texting service instead
    d. The Foundation reserves the right to access, review, copy, delete, disclose, instant messages sent or received via a Foundation phone or other device. Such messages could form part of a Subject Access Request (SAR)
    e. Information that identifies pupils, parents or other members of staff must be kept to a minimum in instant messages and personal information avoided.

28. Disciplinary action may be taken against staff and volunteers who contravene these guidelines, in accordance with the Dean Close Foundation disciplinary procedures.

29. If you require advice on the use of these guidelines, please contact the IT department or a member of the appropriate SLT.

Appendix A – Acceptable Use of IT Policy for Staff (W056)

Staff Summary and Acknowledgement

This appendix summarises the key points of the full Acceptable Use of IT for Staff Policy (W056). It does not replace the full policy, which you should read in full and refer back to as needed. By signing below, you confirm that you have read, understood, and agree to comply with the policy.

1. Scope and legal compliance

- Applies to all employees, peripatetic staff, volunteers and any adult using Foundation IT facilities.
- You must comply with relevant legislation and statutory guidance, including data protection law, the Computer Misuse Act 1990, the Online Safety Act 2023, and current safeguarding guidance (Keeping Children Safe in Education / Working Together to Safeguard Children).
- Using Foundation IT systems means you agree to this policy. Breaches may be treated as a disciplinary matter.

2. Acceptable use

- Foundation IT and internet access is provided primarily to support work – communication with colleagues, parents, pupils and other organisations, and reasonable personal use during the working day.
- Always behave professionally online, exactly as you would in person, by letter or by phone.
- Respect the privacy of others – do not share photos, videos or contact details without appropriate consent.
- Do not use personal email or social media to contact pupils or parents.

3. Not acceptable

- Harassment of any kind; accessing obscene, hateful, pornographic or illegal material.
- Sharing passwords, bypassing filtering/security systems, or using an unauthorised VPN.
- Downloading unlicensed software or copyrighted material; peer-to-peer or BitTorrent use.
- Revealing confidential Foundation, staff or pupil information online.
- Introducing malicious software or undertaking activity that disrupts the network.

4. Monitoring and passwords

- The Foundation monitors use of its IT systems, including internet traffic, sites visited and email content, and may block inappropriate websites.
- Reports on network use are reviewed by the Designated Safeguarding Lead (DSL).
- Keep your username and password private; change your password periodically and do not reuse it across other services.

5. Email

- Send official communications from your Dean Close email address only.

- You are responsible for all mail sent from your account; forgery, junk mail and chain letters are prohibited.
- Do not open messages or attachments from unknown senders.
- Emails (including internal ones) may need to be disclosed as part of legal proceedings, such as a Subject Access Request.

6. Social media

- This policy applies to personal and business use of social media, at any time, on any device.
- Do not speak on behalf of the Foundation or School without permission from the Head.
- Do not discuss or post about pupils, colleagues or the Foundation, or post images including pupils.
- Do not initiate or accept friend requests from current pupils on personal accounts.
- Breach of the social media policy may lead to disciplinary action, including dismissal, regardless of whether Foundation equipment was used.

7. Instant messaging (e.g. WhatsApp)

- The same content standards that apply to email and social media apply to instant messages.
- Only join a messaging group with pupils for a specific, work-related reason (e.g. a trip or team), and make sure your line manager is aware.
- Messages sent or received on a Foundation device may be reviewed by the Foundation and could form part of a Subject Access Request.
- Keep personal information about pupils, parents and staff to a minimum in messages.

8. Consequences

- Failure to comply with this policy, or any related Foundation policy, may result in disciplinary action, up to and including dismissal.
- If you have any questions about this policy, contact the IT department or a member of the appropriate SLT.

Staff Declaration

I confirm that I have read and understood the Dean Close Foundation Acceptable Use of IT for Staff Policy (W056), including this summary appendix, and I agree to comply with its terms at all times.

Full name:	
Job title:	
Department:	
Signature:	
Date:	

(the staff declaration may be completed via an online form or link)