The Athelstan Trust
IT Acceptable Use Policy

Date of Review	Approved by	Date of Approval	Next Review Date	Website
May 2018, May 2021 May 2024	Board	23/5/24	May 2027	Yes

1 **Introduction:** 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:

1.1 The Trust's email and internet services.

1.2 Telephones

1.3 the use of mobile technology on Trust premises or otherwise in the course of your employment (including 4G / 5G, Bluetooth and other wireless technologies) whether using an Academy, Trust or a personal device; and

1.4 any hardware (such as laptops, tablets, printers, mobile phones or teams phones) or software provided by, or made available by, the Trust.

This policy also applies to your use of IT and accessing Trust IT system 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 academies are put at risk.

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

3 **Property:** You should treat any property belonging to the Trust with respect and reasonable care and report any faults or breakages immediately to the IT office and Finance Office. 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.

4 **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. All staff need to ensure that the IT team complete a check of any software / platform / app before it is installed, and a DPIA assessment completed.

5 **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:

5.1 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.

5.2 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.

5.3 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

5.4 All staff logins require Multil factor authentication (MFA), via Microsoft Authenticator, and this will be triggered on any device that is not a school device. This is done to help protect login security and the safety of the data we hold.

6 **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.

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

Internet

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

9 **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 14 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.

10 **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 Headteacher whilst allegations of unsuitable use are investigated by the Trust.

11 **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.

12 **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 Academies, without specific permission from the Headteacher. This applies both to "free" and paid for contracts, subscriptions and Apps. All staff need to ensure that the IT team complete a check of any software / platform / app before it is installed, and a DPIA assessment completed.

13 **Retention periods**: The Trust keeps a record of staff browsing histories for a period of 90 days.

Email

14 **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.

15 **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.

16 **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.

17 **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.

18 **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. See also clauses 16 and 17 above.

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

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

21 **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

22 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. Staff should be aware that the Trust may monitor the contents of a communication (such as the contents of an email).

23 The purposes of such monitoring and accessing include:

23.1 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

23.2 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.

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

25 The Trust also uses 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).

26 The monitoring is carried out by the IT Manager. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Headteacher and CEO and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

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

- Code of Conduct;
- Social Media Policy for Staff
- Data protection policy;
- Information security policy; and
- The School Acceptable use policy for pupils