ELECTRONIC SYSTEMS AND INFORMATION POLICY

Date Agreed:	**June 2021**
Review Date:	**June 2023**
Type of Policy:	**DCAT Non - Statutory Policy**

Revision Number	Date Issued	Prepared by	Approved	Personalised by school	Comments
3	June 2021	DCAT	Trust Board		DPO/GDPR Sentry/JUDICIUM
2	June 2020	CF	DCAT		JUDICIUM
1		SJP/DC	DCAT		DPO

Type of Policy	*Tick* ✓
DCAT Statutory Policy	
DCAT Non-statutory Policy	✓

The March CE Primary School

Contents

Introduction

Our **vision** for our Trust is we exist to:

Help every child achieve their God-given potential

Our **aims** are clear. We aim to be a Trust in which:

Developing the whole child means pupils achieve and maximise their potential

Continued development of staff is valued and improves education for young people

All schools are improving and perform above national expectations

The distinct Christian identity of each academy develops and is celebrated

Our work as a Trust is underpinned by shared **values**. They are taken from the Church of England's vision for Education and guide the work of Trust Centre team. They are:

Aspiration
I can do all things through Christ who strengthens me
(Philippians 4 vs 13).

Wisdom
Listen to advice and accept discipline, and at the end you will be counted among the wise
(Proverbs 19 vs 20)

Respect
So in everything do to others what you would have them do to you
(Matthew 7 vs 12)

Our vision of helping every child achieve their God-given potential is aligned with the Church of England's vision for education and is underpinned by the Bible verse from John: *I have come that they may have life, and have it to the full.*

1. Policy Aims

The Trust'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. It is provided for guidance to all members of staff at the School/Trust who are required to familiarise themselves and comply with its contents. The School/Trust reserves the right to amend its content at any time.

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

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

Staff are referred to the Trust's Data Protection Policy for further information. The School/Trust 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.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School/Trust's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Trust's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

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

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device tablets), and voicemail, but it applies equally to the use of copiers, scanners, and the like.

The Trust is the registered Data Controller, however, most information will be stored at School level and therefore the terms "Trust" and "School" should be interchangeable throughout this policy.

2. 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 6 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Trust/Headteacher who will liaise with the IT provider as appropriate and necessary. Any member of staff who discloses their password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust'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 the School/Trust e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off or lock when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Headteacher or a member of staff from the Trust Centre Team and/or the School Business Manager 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 or lock and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off or locking prevents another member of staff 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 the Headteacher.

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. The School/Trust reserves the right to require employees to hand over all School/Trust data held in computer useable format.

Members of staff who have been issued with a smart phone, laptop, iPad (or other mobile device tablet), 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 machine 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.

3. Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the School/Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the Trust/School's, 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 Head who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers and games, files and opening any documents or communications from suspicious or unknown origins.

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

No device or equipment should be attached to our systems without the prior approval of rge Head or Senior Leadership Group. This includes, but is not limited to, any telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infra-red connection device or any other device.

The School/Trust 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 Lead should be informed immediately if a suspected virus is received. The School/Trust 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. The School/Trust 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 the School/Trust'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 the Trust's Systems and guidance under "E-mail etiquette and content" below.

4. 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.

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

Staff are strictly prohibited from using the School/Trust's email facility for personal emails at any time.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The School/Trust 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 the School/Trust'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. 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. Where it is appropriate for information retention to keep paper copies; relevant e-mails should be printed and retained in 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 the School/Trust. 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 the School/Trust in the same way as the contents of letters.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. 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.

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 Group 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 the School Business Manager who will usually seek to resolve the matter informally. You should refer to the staff handbook for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the Trust's formal grievance procedure. (Further information is contained in the Trust's Staff Handbook and the Grievance Policy and Procedure.)

As 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 the School/Trust;
- 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 or 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;

The School/Trust 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. 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. Business Manager should be informed as soon as reasonably practicable.

5. Use of the web and 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 the School/Trust, 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 therefore access from the School/Trust's system any web page or any files (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 the School/Trust (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School/Trust'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/Trust 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.

The School/Trust's website may be found at https://dcat.academy/. This website is intended to convey our core values and excellence in the educational sector. All members of staff are

encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Group in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The School/Trust has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the School/Trust and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the School/Trust. Any exceptions to this must be authorised by the Head who will liaise with the Senior Leadership Group as appropriate and necessary.

Personal use of the Trust's systems

The School/Trust permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

(a) Use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);
(b) Personal e-mails must be labelled "personal" in the subject header;
(c) Use must not interfere with business or office commitments;
(d) Use must not commit the School/Trust to any marginal costs;
(e) Use must comply at all times with the rules and guidelines set out in this policy;
(f) Use must also comply with the Trust's compliment of operational policies and procedures including but not limited to, the Equal Opportunities and Diversity Policy, Anti-Harassment and Bullying Policy, Data Protection Policy and Code of Conduct.

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 the School/Trust'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.

The School/Trust 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

6. Inappropriate use of equipment and systems

Incidental/occasional/reasonable// personal use is permissible provided it is in full compliance with the School/Trust's rules, policies and procedures (including this policy, the Equal Opportunities and Diversity Policy, Anti-Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

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 the Trust'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):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) Transmitting a false and/or defamatory statement about any person or organisation;
(c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
(d) Transmitting confidential information about the School/Trust and any of its staff, students or associated third parties;
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School/Trust;
(f) Downloading or disseminating material in breach of copyright;
(g) Copying, downloading, storing or running any software without the express prior authorisation of the Head;
(h) Engaging in on line chat rooms, instant messaging, social networking sites and on line gambling;
(i) Forwarding electronic chain letters and other materials;
(j) 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 the School/Trust 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.

7. Cyber Crime

All staff need to be aware of cyber crime and cyber security.

The Trust and the Schools within it, retain responsibility to be aware of the risk of fraud, theft and irregularity and address it by putting in place proportionate controls.

7.1 Overview

Cyber crime is criminal activity committed using computers and/or the internet. It can involve malicious attacks on computer software, including:

7.2 Email hacking

Email hackers try to gain access to email accounts by tricking people to:

- Open and respond to spam emails
- Open emails with a virus
- Open phishing emails

7.3 Phishing

Phishing messages look authentic with corporate logos and a similar format to official emails.

Sometimes phishing emails use the title of a genuine email that the victim has recently replied to in order to trick the victim into believing the communication is authentic. Phishing emails can appear to have originated from within or outside your organisation.

Unlike official communications, phishing emails ask for verification of personal information, such as account numbers, passwords or date of birth.

Sometimes the emails suggest the request is time sensitive to pressure the recipient to respond when they might not otherwise have done so.

Unsuspecting victims who respond may suffer stolen accounts, financial loss and identify theft.

7.4 Malvertising

Malvertising can compromise computers by downloading malicious code when people hover on or click on what looks like an advert. Some will even download malicious code to

your computer while the website is still loading in the background. Cyber criminals can use advertisements as a way to hack into computers.

7.5 Cyber crime: what the Trust can do

To address the risk of fraud, theft and/or irregularity, the Trust will endeavour to:

- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access

The Trust will train staff to ensure that they:

- Check the sender of an email is genuine before, for example, sending payment, data or passwords
- Make direct contact with the sender (without using the reply function) where the email, for example, requests a payment or change of bank details
- If telephoning the sender to confirm authenticity, do not use the contact number within the email without first checking it is genuine
- Understand the risks of using public Wifi
- Understand the risks of not following payment checks and measures

8. Related Policies

Staff should refer to the following policies that are related to this Electronic Systems and Information Policy.

- Data Protection Policy
- Data Breach Policy
- Data Retention Policy
- CCTV Policy
- Information Security Policy
- Freedom of Information Policy
- Privacy Notices