ACCEPTABLE USE POLICY - WORKFORCE

for adoption by all CDAT schools

This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

'Blessed are those who act justly, who always do what is right'

Psalm 106:3

Approved by	Date	Review Schedule	Date of next review
Trust Board	20 December 2023	Annually	Autumn Term 2024

Contents

Introduction and Scope

The Acceptable Use policy includes accessing cloud services on personal devices and governs the use of Chester Diocesan Academy Trust's corporate network and cloud-based systems that individuals use on a daily basis in order to carry out business functions.

This policy applies to all employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school.

This policy should be read in conjunction with the other policies in our information governance policy framework, including the Data Protection policy, Information Security policy and Records Management policy.

Email and Internet Use

We provide email accounts and internet access to the workforce to assist with performance of their duties. We also allow the workforce to use its instant messaging service. For the benefit of doubt Instant Messages are classed as email communications in this policy.

Personal Use

Whilst email accounts and the internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

- Personal messages or internet usage do not tarnish our reputation, or infringe on business functions.
- Users understand that emails sent to and from corporate accounts are the property of the Trust.
- Users understand that we may have access to their email account and any personal messages contained within.
- Users understand that we may have access to their internet browsers and browsing history contained within.
- Users understand that emails sent to or from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation.
- Users understand that we reserve the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network.
- Users understand that we reserve the right to suspend internet access at any time.

Inappropriate Use

We do not permit individuals to send, forward, or solicit emails, or use the internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes or movie files,
- Unwelcome propositions, profanity, obscenity, slander, or libel,
- Any messages or content containing ethnic, religious, political, or racial slurs,
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use emails or the internet to carry out their own business or business of others. This includes, but is not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of Trust management.

Security

Users will take care to use their email accounts and the internet in accordance with our Information Security policy. In particular users will:

- Not click on links from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise our IT network,
- Not send excessively large email attachments without authorisation from management and our IT provider.

Group Email Accounts

Users may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of a user's email rights.

The Trust's Single Point of Contact (SPOC) will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

We may monitor and review all email traffic that comes to and from individual and group email accounts.

Social Media Use

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. We also recognise that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts

We have a number of social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about the Trust and its schools. Authorised users will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. The Trust's SPOC will have overall responsibility for allowing access to social media accounts.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs,
- Be construed as sexually explicit,
- Be construed as political beliefs or commentary.

Personal Accounts

We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach our clients, customers, or partners.

Telephone and Video Conferencing Use

We provide users with access to telephone and video conferencing services to assist with performance of their duties.

Personal Use

Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

- Usage does not tarnish our reputation or infringe on business functions,
- Users understand that we may have access to call history and recordings,
- Users understand that we reserve the right to suspend telephone and video conferencing usage at any time,
- Telephone call or video conference recordings or transcripts may have to be disclosed under Freedom of Information and/or Data Protection legislation.

Inappropriate Use

We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use these services to carry out their own business or business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of Trust management.

Appendix One – Accessing cloud services on personal devices

Introduction

As remote working continues to develop, there has been a move by many organisations to transfer their locally held data into the cloud, enabling access by any internet connected device, anywhere in the world. This brings many benefits to the school, including being able to access data promptly, individuals can use a device of their own choice, and making financial savings as we do not have to provide our own devices to users.

However, with this enhanced access and benefits comes a high level of risk that the school needs to consider and mitigate through the use of technical controls, expected behaviours and supporting policies. This policy aims to provide the framework for adequate management of the risks posed should users access school systems through a non-school provided device.

Personal Devices

We identify a personal device as any electronic device that has not been provided by us and can be used to access and process personal data, including data accessed from the cloud through an internet connection. This includes, but it not limited to:

- Laptop or PC
- Notebook
- iPad or tablet
- Smartphone

Use of the device must be limited to the individual user, and not be shared resources (e.g. a family device).

Permitted Activity

Whilst using their own devices, users are permitted to access, review and process personal data within the school system in which it is held. Users must only access data they are entitled to in order to fulfil their duties.

It is not permitted for any school data to be downloaded and saved onto any personal device under any circumstances. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within our records management system for its full lifecycle, including secure destruction in line with our retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require users to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

Device Security

Anti-virus and software security patching

The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the user to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

We require that any device used for accessing school systems in the cloud must have adequate anti-virus software. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that is going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

Password/PIN protection

All devices must be secured by a unique password or security pin to ensure that access to the device is limited to the named user permitted to access the school's personal data. Devices that lack the ability to enforce this level of security must not be used to access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. Having a robust password or PIN in place provides an additional layer of protection.

Personal applications (apps)

Users are asked to be mindful of the apps installed on personal devices that are used to access school data. Some of these apps may have enhanced privileges and tracking within them that monitor use of the device and other items that are being accessed. This should be detailed in the application's terms and conditions and the user should seek assurance that this risk is being effectively managed.

Equipment disposal

When a device being used to access school information is disposed of, it is the responsibility of the user to ensure that no records or school data have found their way onto the device, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

Physical security

Users should ensure any device used to access school data is kept safe and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, or transported without sufficient protection to prevent accidental damage.

System and Accounts Security

When accessing data held in the cloud via an internet connection (e.g. Microsoft 365), users must ensure that their account is closed when not in use by logging out of the system. It is not permitted for accounts to be left open when not in use, if accessing school systems.

Users are responsible for ensuring any internet connection used to access school data is secured through the use of access controls, such as using a designated username and password. Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

Data Breaches

In the event of a data breach users must follow the process detailed in the Information Security policy and report any suspected breach immediately.

Users are asked to be mindful of the following situations in which the risk of a data breach increases:

- Systems are not shut down appropriately when not in use, leading to unauthorised access of school data.
- Personal devices are shared with family, friends, or partners leading to unauthorised access of school data.
- Documents and files are downloaded onto shared devices, and then become accessible to other users of the device.
- Passwords or security PINs are shared with others (e.g. family and partners) leading to unauthorised access of school data.
- Inadequate management of security and software updates leaves a vulnerability to a virus or hack. Once unauthorised control of a device is established it is difficult to identify and remove.
- Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.

Authorised Access

Access to school systems using personal devices is only permitted whilst the user has authorisation to do so. In the event that the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as a data breach and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left our employment.

Exemption Process

An exemption to any element of this policy can only be authorised by the school's Senior Information Risk Owner (SIRO). Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.