City Gateway

Safer Communication in City Gateway Policy

Reviewed by (name)	Date	Next review needed
Diane Betts	February 2022	February 2023
Mark Pike	November 2022	November 2023
Diane Betts	January 2023	January 2024

This policy will be reviewed on an annual basis

Contents

SAFER COMMUNICATION IN CITY GATEWAY COMMUNITY POLICY

This Communications Policy applies to all staff and volunteers ("Users") of young persons at City Gateway who use the communications equipment and systems provided by the Company.

Users are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.

In light of the fact that communications made by Users reflect upon the Company and are capable of creating a number of commercial, professional and legal problems, this policy is intended to clarify what the Company expects from Users and their responsibilities when using the Company's communications facilities.

Communications equipment include Telephone; Email; Internet and Intranet (SharePoint); And any other communication device or network provided by the Company.

Whilst the communications equipment and systems provided by the Company are made available to Users for the purposes of the business, a certain amount of limited personal use is permitted insofar as such personal use is consistent with this Communications Policy and the duties of the User.

If a machine is not in use, it can be removed from scope.
All active machines are updated within 14 days.
If a dormant machine is to be brought back into use, there is a documented process that is implemented when re-activating the dormant machine and this includes applying all latest updates.

General Principles

There are certain general principles that should be born in mind when using any type of communication, be it external or internal, including hard copy letters and notices. We take our responsibility seriously with regard to radicalisation and extremism and promote integration and British Values throughout the organisation which is therefore integral to all our communication systems.

The Company expects all Users to:

- Use communications equipment and facilities responsibly and professionally, and at all times in accordance with your duties, including Company letterheads and stationery.
- Be mindful of what constitutes confidential or restricted information and to ensure that such information is never disseminated in the course of communications without express authority.

- Respect and support British Values. Be responsible when communicating respecting other people's rights to safety; not to hurt or abuse others and not to threaten to hurt or abuse others.
- British Values are: -
    - Democracy
    - The rule of law
    - Individual liberty and mutual respect
    - Tolerance of those with different faiths and beliefs.
    - Always be aware of and show respect to other users.
    - Ensure that they do not breach any copyright or other intellectual property right when making communications.
    - Ensure that they do not bind themselves or the Company to any agreement without express authority to do so.
    - Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Company and conduct their use of communication systems and equipment accordingly.

Internet

The Company provides access to the internet for the sole purpose of business and to assist Users in the furtherance of their duties.

We have safeguards in place to prevent access to unsuitable content and websites for staff and volunteers' safety.

The Company recognises that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and does not interfere with the User's performance of their duties and is outside of normal working hours or during a lunch break.

Users must not use the internet to gain or attempt to gain unauthorised access to computer material or private databases, including restricted areas of the Company's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus or other malicious software or code to or using the communications equipment or systems of the Company.

Users must not access or attempt to access any information which they know or ought to know is confidential or restricted.

Users must not download or install any software without the express permission of the Chief Executive.

Certain websites are blocked and cannot be accessed from the Company's equipment or systems. If a User has a genuine and specific business need to access a blocked site, they must contact the Online Safety Officer who will consider providing an over-ride password.

Users must not attempt to download, view or otherwise retrieve illegal, pornographic, discriminatory or any other material which may cause embarrassment to the corporate image of the Company. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced or withdrawn, may be subject to

disciplinary action or summary dismissal.

Blogging and Social Networking Sites

The viewing of or contribution to personal blogs, content sharing and social networking sites such as "Facebook", "Instagram" "WhatsApp", "Twitter" "Tik Tok" and "YouTube" using the Company's communications systems is prohibited during working hours. Viewing of these sites for business or training use is acceptable.

The Company recognises that in their private time Users may wish to publish content on the internet through a variety of means. Even outside of work Users must adhere to this policy when creating, modifying or contributing to websites.

If a User makes any posting, contribution or creation or publishes any other content which identifies or could identify the User as an employee, contractor, agent or other member or associate of the Company, or in which the User discusses their work or experiences relating to the Company, the User must at all times ensure that their conduct is appropriate and consistent with their contract of employment and the corporate image of the Company, and should bear in mind that the User as an employee owes a duty of fidelity to the Company.

If a User is unsure as to the appropriateness of a posting or other content published by them, they should speak to their Line Manager at the earliest opportunity to seek clarification.

If, in any contribution or posting which identifies or could identify the User as an employee, agent or other affiliate of the Company, the User expresses an idea or opinion they should include a disclaimer which clearly states that the opinion or idea expressed is that of the User and does not represent that of the Company.

Email

Company Email

The email address with which Users are provided by the Company is provided for business purposes in order to facilitate information sharing and timely communication with clients, customers, colleagues, suppliers, etc. Any Company business should be conducted through the Company email provided upon induction unless otherwise agreed with the User's line manager.

Users should adopt the following points as part of best practice:

- Before communicating via email, Users should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence;
- All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text;
- Emails should be worded appropriately and in a professional manner.

Users must not email any business document to their own or a colleague's personal web-based email accounts, unless required to do so for work purposes. Further, Users must not email any business document to any web-based email address unless specifically

permitted to do so by them.

The Company recognises that there may be instances where Users may need to use their Company email address for personal reasons. This is permitted on the condition that such use is kept to a minimum and does not interfere with the performance of the User's duties. In any case Users are not permitted to use their Company email address to subscribe to any newsletters or to receive any marketing, as this will result in extra unnecessary burden being placed upon the Company's communications systems.

If Users do use the Company email for personal reasons, they will be deemed to agree to the possibility that any emails sent or received may be subject to monitoring in accordance with this policy.

Users should at all times remember that email messages may have to be disclosed as evidence for any court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Company's interests. Users should remember that data which appears to have been deleted is recoverable.

Personal Email

Users are permitted to access and use their personal email accounts only to the extent that such use is reasonable and does not interfere with the User's performance of their duties and is outside of normal working hours or during a lunch break.

Mobile Phones and Desk Telephones

The Chief Executive must approve any business case for any mobile phone.
Staff have a choice of holding a company mobile under a City Gateway contract or to use their own personal mobile for business use. In both cases the limit per month will be capped at £24.50 including VAT for all calls, texts and internet access.

Staff Pay As You Go mobiles must not be used for internet, multimedia messaging, dialling free phone, non-geographic, premium rates or international telephone numbers unless there is a legitimate business need for so doing. Staff must email any use outlined above to their manager, preferably prior to doing any of the above to ensure approval. Where appropriate, a manager may gain prior approval in principle from the Chief Executive for making use of applications or numbers detailed above.

Mobile phones provided for business use by the Company must not be used for personal calls except in emergency. Personal mobile phones must be switched to silent or vibrate during working hours. Where a staff member is not contactable on their Company device (for example, they are driving, or in a meeting), their personal phone number should not be called except in an absolute emergency. The Company provides devices for business use, so that the staff member does not have to use their private phone for work calls.

Users are permitted to use their personal mobile phones only to the extent that such use is reasonable and does not interfere with the User's performance of their duties and is outside of normal working hours or during a lunch break. Use includes phone calls, text messages, accessing the internet, social networking sites, apps and emails, playing music and videos (including the use of earphones). Use is limited to before and after working hours and during authorised breaks.

Only organisation devices should be used to take photographs of organisation activities. The use of camera devices of any sort is not permitted in toilet, washroom or changing areas. Mobile phones must not be used except during break and lunch times in a suitable place and must not be used in front of learners. **The use of personal mobile devices by staff to take pictures is not allowed.**

Staff will be responsible for their company mobile and related accessories. The phones must not be left unattended and should a phone be lost it will be the staff member's responsibility to replace it. The device should be kept out of sight when not in use.

Due to the fact that personal data (as defined by the Data Protection Act) may be kept on mobiles or any other hand-held PDA device, staff must password or PIN protect the device immediately on receipt.

Staff must notify the Head of Finance all current pass codes, id and passwords. This is to make sure that our records are accurate and in case a phone goes missing, we have access to it.

This will include completing and signing the below:

Staff Name _____

Job Title _____

Mobile Phone number _____

Make and model of mobile phone _____

IMEI number (on iPhone's go to Settings, General and About and scroll down to number or alternatively it is displayed (very small) on the back of the phone)

_____

Signed _____

Dated _____

I have read and understood the use of Mobile Phones as explained under the section **Mobile Phones and Desk Telephones** and will return all City Gateway property including chargers when required.

Signed…….. Dated……..

Desk Telephones

Desk telephones are provided to enable staff members to perform their duties and to conduct the business of City Gateway.

The use of the internal telephone to contact staff directly should always be used initially as these calls attract no cost.

Calls to staff members' company mobiles should only be made if they are not contactable through the internal telephone system.

Local calls made from desk landline phones are totally at the discretion of the staff member and it is the responsibility of each staff member to ensure calls are appropriate to their work and are conducted expeditiously. Private calls are not permitted except in emergency situations. All international calls are strictly prohibited.

All numbers are monitored and Finance receive a monthly report detailing all calls. The cost of calls will be charged to any individual who misuses the telephone system. Any User found to be misusing the communications equipment and systems provided by the Company will be treated in line with the Company disciplinary procedure.

In accepting a City Gateway desk telephone staff members acknowledge the right for City Gateway to list their names in its telephone or other associated directories (including the internet and intranet) and to have their extension number and calling party displayed.

The following is relevant for those with a mobile or landline phone ONLY. We need to ensure we have some consistency around the message we give to anyone who is not able to get hold of you.

Firstly, please ensure you set a personalised answerphone message on your phone and not the generic one that comes with it.

Secondly, please use one of the below messages to record a personalised message;

Option 1 - Thank you for calling <your name> at City Gateway. I am sorry I am unable to take your call right now but please leave a message and I will get back to you as soon as possible. If your call is urgent please try our head office number on 0203 727 6310. Thanks.

Option 2 - Thank you for calling <your name> at City Gateway. I am sorry I am unable to take your call right now but please leave a message and I will get back to you as soon as possible. If your call is urgent please contact my colleague <colleague's name> on <colleague's number>. Thanks.

Absence hotline – Thank you for calling the absence hotline. Please leave a message with your name, lessons you will be missing and reason for your absence. Please also leave your phone number so we can call you if we need. Thanks

If you are on annual leave please adjust your message accordingly;

Option 3 - Thank you for calling <your name> at City Gateway. I am currently on annual leave returning to the office on <date of return>. Please feel free to leave me a message and I will get back to you on my return to the office or, if your query is urgent, please call <our head office on 0203 727 6310/ my colleague <colleague's name> on <colleague's number>. Thanks.

Security

The integrity of the Company's business relies on the security of its communications equipment and systems. Users bear the responsibility of preserving the security of communications equipment and systems through careful and cautious use.

Access to certain websites are blocked from Company communications equipment and systems for Users' safety. Often the decision to block a website is based on potential security risks that the site poses. Users must not attempt to circumvent any blocks placed on any website or features by the Company unless authorised to do so by the Online Safety Officer (Head of Education and Inclusion).

Users must not download or install any software or program without the express permission of the Online Safety Officer.

Users must not share any password that they use for accessing Company communications equipment and systems with any person, other than when it is necessary for maintenance or repairs by IT Contractors. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by IT. Users are reminded that it is good practice to change passwords regularly.

Users must ensure that confidential and sensitive information is kept secure. Workstations and screens should be locked when the User is away from the machine, hard copy files and documents should be secured when not in use and caution should be exercised when using mobile telephones outside of the workplace.

When opening email from external sources Users must exercise caution in light of the risk viruses pose to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus they must notify the IT Contractor.

No external equipment or device may be connected to or used in conjunction with the Company's equipment or systems without the prior express permission of the IT Contractor.

Monitoring

The Company may monitor Users' communications for the following reasons:

- To ensure Company policies and guidelines are followed, and standards of service are maintained;
- To provide evidence of transactions and communications;
- To help combat unauthorised use of the Company's communications equipment and systems and maintain security;
- In order to better understand the requirements of the Company in terms of the provision of communications equipment and systems.

Users should be aware that all internet and email traffic data sent and received using the

Company's communication systems may be logged, including websites visited, times of visits and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using the Company's communications equipment and systems for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of communications complies with the Data Protection Act 1998.

Misuse and Compliance

Any User found to be misusing the communications equipment and systems provided by the Company will be treated in line with the Company disciplinary procedure.

The viewing, transmission, downloading, uploading or accessing in any way any of the following material using Company communications equipment and systems will amount to Gross Misconduct with the possibility of summary dismissal, and when necessary be reported to the police:

- Material which is pornographic, sexist, racist, homophobic, paedophilic or any other discriminatory or otherwise offensive;
- Illegal or criminal material, including material which breaches copyright or any other intellectual property right;
- Any material which has the object or effect of causing harassment to the recipient;
- Material which the User knows or ought to know is confidential or restricted information and which they are not authorised to deal with;
- Any website which the Company has blocked access to from the Company communications equipment and systems.

Consequences of Misuse of Email Facilities

Respect & British Values. Respect must always be given to other people's rights to safety; not to hurt or abuse others and not to threaten to hurt or abuse others. We also take our responsibilities seriously with regard to radicalisation and extremism. We have safeguards in place to prevent access to unsuitable content and websites and any breach will be considered under our Disciplinary Procedure.

Discrimination. Any material disseminated which is discriminatory or encourages discrimination may be unlawful under the Sex Discrimination Act 1975, the Race Relations Act 1976 or the Disability Discrimination Act 1995 where it involves discrimination on the grounds of sex, race or disability.

Data Protection. Processing information (including photographs) which contains personal data about individuals, requires the express written consent of those individuals. Any use of personal data beyond that registered with the Data Protection Commissioner will be illegal.

Defamation. As a form of publication, the internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the

sender of the email and may lead to substantial financial penalties being imposed.

Obscenity. A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.

Intellectual property. Anyone who uses email to send or receive any materials that infringe the intellectual property rights of a third party may be liable to that third party if such use is not authorised by them.

Online Safety

There is evidence that some websites, including those used for academic purposes, are accessed by users who wish to exploit others with a view to compromising personal safety and private information. Users are advised to exercise care when communicating through the internet with people they do not know personally.

The following guidelines should be followed:

- Never arrange a meeting alone with someone you have made contact with on the internet;
- Never disclose any personal information through the internet to unknown persons or organisations;
- Be aware that any unknown persons you are communicating with through the internet may not be who you think they are and photographs they display may not be their own;
- Speak to a senior member of staff if you are concerned about your online safety inside and outside of City gateway.
- Make a senior member of staff aware if you have been threatened online.

Substantive Social Media Offences

Users must be aware of the acceptable use of social media. The following are potential offences:

- Harassment or stalking;
- Controlling or coercive behaviour;
- Blackmail;
- Juror misconduct;
- Contempt of court;
- Publishing material which may lead to the identification of a complainant of a sexual offence;
- Intimidating a witness or juror;
- Breach of automatic or discretionary reporting restrictions;
- Breach of a restraining order;
- Disclosing private sexual images without consent;
- Causing sexual activity without consent, or causing or inciting a child to engage in sexual activity, or sexual communication with a child;
- Taking, distribution, possessing or publishing indecent photographs of a child;

- The act of setting up a false social networking account or website, or the creation of a false or offensive profile or alias could amount to a criminal offence, depending on the circumstances;
- A "photoshopped" (digitally edited) image of a person is created and posted on a social media platform. Although many photoshopped images are humorous and inoffensive, others are disturbing or sinister, such as the merging of a person's face with the nude body of another to create obscene images, which may be accompanied by offensive comment.

Passwords

It is important to ensure that all passwords that you use, inside and outside of City Gateway are created and kept as secure as possible.

A strong password should:

- Be at least 12 characters long;
- Not contain any of your personal information such as your real name, user name, or names of friends or family;
- Be very unique from your previously used passwords;
- Not contain any word spelled completely;
- Contain characters including: uppercase letters, lowercase letters, numbers, and characters.

Do not use the same password for different applications (e.g. online banking, shopping, medical, social media, etc)

City Gateway are using Azure AD Connect to sync their Azure based domain to Microsoft 365. Accounts are therefore controlled by a password policy on the domain. The password policy states the following:
24 passwords are remembered
Max age – 42 days
Min age – 1 day
Min length – 12 characters
Password complexity is required.

Use of the Internet – Filtering

All internet activity is monitored by City Gateway for security and personal safety purposes, and it is possible to identify individual usage. City Gateway reserves the right to search internet accounts accessed with company equipment without permission if it is felt that illegal or otherwise inappropriate use of technology is occurring.

By accessing the internet from City Gateway's network, you agree to the terms and conditions of City Gateway's Network Acceptable Use Policy as follows:

City Gateway provides internet access to assist you in your training. This policy cannot define every specific coursework related use of the internet. Examples of acceptable use

include research for assessments, using online learning materials, job searching, uploading CV's or participating in forums or online groups appropriate to your course. You are asked not to abuse this privilege. Any abuse may result in the withdrawal of Internet access and, in the event of a serious breach, will lead to disciplinary procedures.

Some areas of the internet contain information, in textual or graphic form, which could cause offence to other people or may be illegal to download or view. You are prohibited from knowingly accessing, viewing or downloading such material.

You must not bring City Gateway into disrepute through the use of online social networking activities.

Examples include uploading images or videos which show antisocial behaviour or illegal activities; making derogatory statements about City Gateway, City Gateway staff or other learners; or revealing confidential information about City Gateway, City Gateway staff or other learners. This list is not exhaustive.

You must not use images of City Gateway offices or staff, or City Gateway's logos, in videos or photographs, without prior permission from the Head of Marketing.

You are not permitted to download and/or install software.

You are not permitted to attempt to remove software that has been installed on City Gateway network by the IT contractors.

City Gateway reserves the right to withdraw internet access for any learner found or believed to be:

- in possession of material which is sexist, racist, abusive, defamatory or obscene;
- in possession of material promoting discriminatory actions or illegal behaviour;
- in possession of material which may lead to learners becoming radicalised or being exposed or drawn to extremism which may include:-
    * Verbal or written support for terrorism
    * Expressions of threat towards the UK defence forces
    * Expressions of intolerance towards other faiths and groups
    * Signs that an individual is embracing and extreme or fundamentalist ideology
    * Accessing extremist content on the internet and/or social media

Online Learning away from City Gateway offices

City Gateway is doing what we reasonably can to keep all of our learners safe whilst accessing learning from home or from other premises. It is important that all staff who interact with learners, including online, continue to look out for signs a learner may be at risk. Any such concerns should be dealt with as per our child protection policy and where appropriate referrals should still be made to children's social care and as required the police.

To support learners access online learning City Gateway will be loaning out laptops. These have been tested to ensure the restrictions are in place to safeguard the young person when connecting to the internet through web-filtering.
Staff should:

- Remind learners about online safety and who to report concerns to.
- Use City Gateway endorsed systems for online learning.
- Not give learners their personal number or personal email.
- Not use their own phone to contact a learner.
- Read, understand and agree the following policies; E Safety, Safer Communication, GDPR and Privacy statements.
- Ensure the live class is recorded via Teams and sent to Head of Marketing to upload. Face Time, WhatsApp or other mobile video platforms are not to be used.

City Gateway will consider recently published guidance from the UK Safer Internet Centre on safe remote learning and from the London Grid for Learning on the use of videos and livestreaming when planning online lessons and/or activities and plan them safely.

City Gateway will always consider the safety of their learners when they are asked to work online. The starting point for online teaching will be that the same principles as set out our staff behaviour policy, acceptable use of IT equipment policy, safer communication policy including the use of social media.

The principles set out in the guidance for safer working practice for those working with children and young people in education settings published by the Safer Recruitment Consortium will also be considered to ensure our policies are robust and effective.

City Gateway will ensure any use of online learning tools and systems is in line with privacy and Data Protection/GDPR requirements and City Gateway Data Protection Policy.

Video conferencing

Staff may be using video technology to interact with learners e.g. Teams within Office 365. We can continue to communicate via WhatsApp but this must not be a video or face to face communication but text message only.

Staff (and learners where appropriate) should

- Avoid video 1:1s. There MUST always be 2 staff members invited unless the meeting is recorded in full.
- Always use a City Gateway phone or device if they have one. These are monitored.
- Use City Gateway permitted communication channels (Teams in Office 365).
- Ensure learners wear suitable clothing, as should anyone else in the household.
- Use computers in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- Ensure live classes are kept to a reasonable length of time. Learners may also have to respond to their families during this time.
- Ensure language is professional and appropriate, including any family

Safer use of Zoom Video Conferencing for learner and/or staff interaction

- Use a new meeting room each time (i.e. don't use the personal meeting ID)
- Don't allow attendees to join before host

- Mute attendees on joining
- Turn screen sharing off
- Set up a 'waiting room'
- Lock your meeting room after you have started
- Don't publicise your meeting's link on social media
- Don't share the screenshot of everyone, especially when it shows the meeting ID
- Try to have someone whose job it is to 'manage the room' and focus just on doing that.
- Tell people what the Plan B is (i.e. if you do have to abort the meeting where will the meeting move to and how can people re-join)
- Avoid sharing personal information
- Turn off your video and microphone unless it's needed.

Trustee Meetings (full Board and Committees)

- Cameras must be on at all times.
- Trustees should sign in using their own identification.
- Attendance should be in a room without others being present