LONDON FIRE BRIGADE

ICT acceptable use policy

New policy number:	**485**
Old instruction number:	
Issue date:	**18 April 2012**
Reviewed as current:	**3 July 2020**
Owner:	**Chief Information Officer**
Responsible work team:	**ICT Security Manager**

Contents

1 Introduction

1.1 This acceptable use policy (AUP) sets out policy requirements for the use of the Brigade's ICT.

1.2 There are a number of risks to the Brigade which arise from use of the Brigade's ICT. For example, a phishing email attempting to introduce a damaging computer virus to the Brigade's network; a mobile device along with the Brigade's data stored on it being lost or accessed by an unauthorised person; the Brigade's data being intercepted between sending and receiving; or a breach of law (e.g. copyright law).

1.3 The Brigade's ICT is diverse and ranges from desk terminals and PCs, laptops, tablets and mobile and fixed line telephones to enterprise infrastructure, as well as externally hosted Cloud[1] solutions.

1.4 When making use of the Brigade's ICT, clear rules are needed on what is and is not permitted in terms of acceptable use.

1.5 Use of the Brigade's ICT, including the email system and internet access, is foremost to be used for conducting the Brigade's official business and always for lawful purposes.

1.6 This AUP is a mandatory policy for all staff, including temporary staff and contractors working on the Brigade's behalf, and any other users, including third parties, who are granted access to the Brigade's ICT.

1.7 Users will be informed of any changes made to the AUP; staff can find the most up-to-date version on ***hotwire***.

2 Acceptable use and disciplinary action

2.1 Failure to comply with this AUP could lead to disciplinary action being taken against you, under the Brigade's disciplinary procedures, which could result in action up to and including your dismissal. Some actions may also be a criminal offence.

2.2 Failure to comply with the AUP by any third party may result in the suspension of access to the Brigade's ICT computing environment and may constitute a breach of contract.[2]

3 Ten steps to staying secure

3.1 Ten steps to staying secure sit at the heart of a collection of rules, collectively called the AUP, that are necessary to keep the Brigade ICT infrastructure secure and prevent security incidents.

[1] Cloud computing is the storage of and access to data and programs over the internet.

[2] It may also amount to a breach of any 'Third Party Network Access Agreement ' entered into between the Brigade and third party].

Step 1: Everyone is responsible for security

Our people are our greatest defence against the harmful impacts that could result from security incidents. It is important that you understand your responsibilities under this AUP and abide by the rules and follow security advice published by the Brigade at all times.

Goals:

- Everyone who uses the Brigade's ICT facilities understands their security responsibilities.
- Accidental and deliberate breaches and the harmful impacts they can cause are avoided.
- Cyber threats targeting our people are successfully defended.

Description	**Policies**
Your responsibility	It is essential that you understand and observe the requirements set out in this AUP. If you are not clear about any issue, seek guidance from your line manager. If you become aware of actions by other users which do not comply with this AUP or you are affected by the actions of other users which are not permitted, the matter should be reported to your line manager who will decide what further action to take.
Security awareness	All staff are required to complete the security awareness eLearning course. You will need to retake the course every two years.
Follow procedures	Always follow the Brigade's policies and procedures as appropriate to your work, for example, use approved methods for storing, processing and sharing the Brigade's information or for working remotely. The use of systems and services that have not been approved by the Brigade could result in security incidents and harm to the Brigade and are not permitted.
Third party responsibilities	Third party users must always work within the terms and conditions set out in their respective agreements and in accordance with this ICT AUP as applicable. Any third party user who is not clear about any issue must seek advice from the officer within their organisation responsible for their personnel's use of the Brigade's ICT.

Step 2: Don't offend others or break the law

Goals:

- The Brigade complies with its statutory obligations.
- Breaches of licence terms are avoided.
- The Brigade's computing facilities are not abused to cause offence to others.

Description	Policies
Abuse of ICT facilities	Never access, create, store or distribute material that: x Could be harmful to the Brigade's reputation, image or that commits, incites, aids or promotes any criminal activity. x Is discriminatory, abusive, derogatory or otherwise contains language or images that are racist, sexist, homophobic, biphobic, transphobic, obscene, pornographic or sexually explicit, or otherwise in breach of the Brigade's Culture Review which sets out the Brigade's zero tolerance of this type of behaviour. x Bullies, intimidates, or harasses any person contrary to the Brigade's Togetherness policy. x May contain inappropriate content (e.g. pornographic images), viruses or unlicensed software.
Copyright infringement	You must not, in respect of material obtained from external bodies (e.g. via an internet web site or as an email or email attachment) reproduce, download, circulate, copy or scan it unless you are satisfied that it will not breach copyright or that any condition allowing copying is complied with. For further information refer to Copyright information on hotwire.
Licence infringement	You must not: x Attempt to install, use, store or distribute any software or computer programs (including screensavers) not supplied by the Brigade unless explicitly permitted by the chief information officer. However, staff issued a Corporately-Owned Personally-Enabled (COPE) mobile phone may download apps to the phone's personal space, as permitted in Step 9 Follow the rules for personal use, and in doing so are responsible for complying with licence terms and conditions. x Copy any software licensed to the Brigade.
Private accounts	x The Brigade cannot protect data processed using your private accounts which the Brigade does not manage, such as email, file storage and file sharing services and other consumer apps. Use of private accounts for work purposes may result in licence infringements or personal data being exposed to risks. Never use WhatsApp and other private accounts for official business purposes. Policy number 944 - The Brigade's social media policy sets out how to use social media so that harmful impacts to the Brigade and its employees are avoided. Step 9 'Follow the rules for personal use' sets out how the personal space of Brigade-issued Corporately-Owned Personally-Enabled (COPE) phones may be used.

Step 3: Secure data appropriately

Goals:

- Sensitive data is handled correctly.
- Data that is shared with the Brigade's partners remains secure.
- Legal obligations for protecting personal data are complied with.
- LFB data is processed by approved solutions with appropriate security.

Description	Policies
Protecting equipment when not in use	As a matter of good practice: ✓ Always lock your workstation (by pressing Ctrl +Alt + Del then clicking Lock Computer on a Microsoft computer; or Apple Menu and Lock Screen on an Apple computer) or mobile device (e.g. tablets, phones) when not in use or unattended. ✓ Access to Brigade mobile phones must be protected by a PIN or biometrics (e.g. fingerprint recognition). x Never leave an open file or session on your computer/device unattended or unsupervised.
Security Classifications	You are required to ensure that the Brigade's data is handled appropriately by applying an appropriate security classification and ensuring that the data is always handled in the correct way. See Brigade Policy number 619 – 'LFB security classifications system' which defines the security classifications currently in use and handling requirements.
Sharing Brigade data externally	When sharing data externally, always apply the appropriate Security Classification (see above) and use the Brigade's approved methods for sharing information. The Brigade's sensitive information exchanged with external parties must be transmitted using the Brigade's approved secure email or secure file transfer facilities. Contact the IT Service Desk if you need access to these facilities.
Agile, digital and secure	Digital technologies are constantly evolving. ✓ Always ensure you use solutions approved by the Brigade. x The informal or ad hoc use of unapproved Cloud services[3] (e.g. data storage using online services that are not managed by the Brigade) exposes the Brigade to risks and is not permitted.
Keep business and personal separate	x Never use private accounts or storage for working with or storing the Brigade's data unless the information is of a nature suitable to be in the public domain and you have written authorisation from the chief information officer.

[3] Cloud services include online applications, data storage, social media and other websites accessed over the internet.

Step 4: Protect your identity

Goals:

- Information is accessed by authenticated users.
- Impersonation of authorised users is avoided.
- Social engineering is unsuccessful.

Description	**Policies**
Choosing passwords	You must not: x Base passwords on things that other users might know (like birth dates, family names, telephone numbers, football team, holiday destination or a series of the same or sequential characters/numbers). ✓ You are advised to use strong passwords (such as three random words) which are unique with each account that you use.
Keeping your passwords safe	You must not : x Disclose or share your password with any other person. x Keep a paper record of the password, unless it is stored securely (e.g. as you would store your banking PIN).
Don't become accountable for someone else's actions	You must not: x Allow anyone else to use a computer you are logged on to with your own personal account. x Attempt to gain unauthorised access to the Brigade's computer system using another person's user ID and password. As a matter of good practice: ✓ Change your password if you believe it may have been breached or become known by another person.
Protecting your online identity	Don't make it easy for criminals to gather your logon credentials or other information about you which could be used to target the Brigade or it partners. Even a strong password is useless if it is harvested by criminals from an insecure website. ✓ Be alert to phishing emails and always follow related advice issued by the Brigade. Particularly, never open attachments or click on links that you are not expecting. Check by calling a trusted phone number if you receive an unexpected link or attachment from someone you know. ✓ Always use a unique password with each online service. Changing just the last one or two characters is not effective protection as criminals copy common habits and try such variations. ✓ You are advised to check the privacy settings with your social media accounts and avoid publicly posting private details that could be used by criminals to impersonate you. ✓ It is recommended that you use a second factor of authentication (e.g. a token code generated by the online service) with your private online accounts where available. x Never use your work password for any other service, not even for online services you sign up to for business use.

Description	**Policies**
Security for mobile phones	You must: ✓ set-up a six digit PIN for your Brigade phone. This PIN must not be easy to guess (e.g. 111111, 123456). You must keep your PIN secret and never share it. You may: ✓ set-up an alternative way to access your Brigade mobile phone in addition to the PIN. It is recommended that you set up the biometric fingerprint and/or facial recognition which provides convenient security and avoids problems such as forgotten PINs and passwords. The 'biometric' information (i.e. fingerprints and face patterns) remains securely on the phone and is not used elsewhere. If you do not want to use the biometric feature, you can instead set up a strong password. The Brigade may, in the future, require you to use an additional biometric feature or password to access the secure work area of the phone. Setting up biometrics or a password provides an added level of security for the business data on the phone.

Step 5: Protect computers and avoid waste

Goals:

- Information systems are available where and when needed.
- ICT facilities are supported.
- Unnecessary and wasteful printing is avoided.

Description	Policies
ICT facilities are managed to Brigade standards	You must not: x Connect personally owned or arrange for another party (e.g. a broadband service provider) to connect any computer equipment to any part of the Brigade's network or computers unless this has been agreed in writing, in advance, by the chief information officer. x Re-locate or remove any ICT equipment between desks, offices or other locations without prior written approval from the ICT Service Desk. x Attempt to repair any item of computer equipment, or remove equipment from casings or any security device. Any problems should be reported to the ICT Service Desk.
Software is supported and compatible	All business software for use on the Brigade's computers must be obtained via the ICT Service Desk. Apps may be downloaded for private use to the personal space of Brigade-issued Corporately-Owned Privately-Enabled (COPE) mobile phones as permitted in Step 9 'Follow the rules for personal use'.
Privileged access only when required	Administrator accounts and other accounts granted special privileges must not be used to perform tasks that could be carried out under a regular network account and/or using a 'thin client' session.
Avoid wasteful printing	Unnecessary printing wastes money through the high cost of paper, toner cartridges and printer maintenance. Avoiding unnecessary printing not only saves money but also reduces environmental impact through a reduction in the use of paper, toner cartridges and electricity. x Avoid non-essential printing, making use of electronic alternatives where appropriate, e.g. promote social events on the 'events' page on ***hotwire***[4].
When travelling abroad	If you are travelling abroad you are advised to consider if you need to take your Brigade mobile device, including your Brigade phone, with you, whether for business or private use. You are advised not to take your phone to a country considered to be high risk or if you do, to keep it on you or locked in your hotel safe. You should check Foreign and Commonwealth Office advice when travelling outside the EEA: https://www.gov.uk/foreign-travel-advice.

[4] ***hotwire*** provides a facility for publishing information to colleagues about social events and activities of clubs and societies approved by the Brigade. Refer to the 'events' page found in '***hotwire*** favourites'.

Step 6: Use email safely

Goals:

- Cyber threats delivered via email are successfully defended.
- Information is shared appropriately.
- Accidental or deliberate data breaches are avoided.
- Email facilities are not abused.

Description	Policies
Don't become a victim of phishing	Be aware of the threat of 'phishing[5]' emails which may appear to be from someone you know, or even from a known sender whose account is under the control of criminals. ✓ You must take care with messages that are unexpected or appear to be from someone you know but not in their usual style. ✓ You can report phishing emails to the 'Phishing' mailbox to help ICT recognise trends or act on threats, but don't report messages that have been safely quarantined. ✓ If you think you have been individually targeted with a phishing email, report it to the IT Service Desk. ✓ Only use your LFB email address for business/professional purposes. x Don't click on links or open file attachments in emails unless you are confident the sender and message are genuine.
Safe use of email	✓ Always follow the advice in Step 3 'Secure data appropriately' when sharing LFB's information externally. You must not use the Brigade's email system: x To make representations or express opinions as being those of the Brigade, except where you are authorised to do so. x To transmit personal[6] data, to your or any other person's private email account (e.g. Hotmail, Google, Yahoo, etc.). In any event, personal data should not be sent to any person or organisation unless you have authority do so, there is a legitimate business need for the recipient to have it, and it is in accordance with the data protection law. x To transmit the Brigade's information to your or any other person's private email account, if it is subject to a Brigade security classification[7] or otherwise contains sensitive information which could adversely impact on the Brigade's reputation if it were to be made public. If in doubt, contact the Brigade's data protection officer for clarification. x To amend any received email message and then forward it on, without making clear any changes you have made. x To distribute chain letter or other mass-circulated, non-business-related, emails including emails promoting social events (e.g. retirement posters)[8]. x To pretend to be another user when sending an email message or to represent yourself as another user on the system. x To access or attempt to access another user's email messages without authorisation.

[5] Phishing is a deceptive attempt to impersonate a sender for malicious purposes.
[6] See Brigade Policy number 351 on data protection for the definition and application of 'personal data'.
[7] See Brigade Policy number 619 – 'LFB Security Classifications System' which defines the security classifications in use. [8] See footnote 4.

Description	Policies
Email good practice	As a matter of good practice: ✓ Always review the contents of emails before sending them. Remember, email messages may be subject to disclosure under the Freedom of Information Act, data protection law and/or the Environmental Information Regulations. ✓ Delete any mass circulated email you receive, without opening it (or any attachment) containing jokes, images, programs or other non-business related content - since they commonly contain viruses. ✓ Identify yourself in every email (including replies) by adding your name, post title, telephone number and location as an auto-signature in line with Brigade policy here. Always make sure that the London Fire Brigade is mentioned in your auto-signature. ✓ Don't use personal 'strap lines', mottos or slogans, at the end of emails. ✓ Take special care when communicating personal data or sensitive information. If such information is attached to an email as a file you should use the Brigade's secure email facility. Contact the IT Service Desk if you need advice. ✓ Take care to make sure that any statements or opinions about other people or organisations are true and in the case of opinions based on fact and genuine. If you receive unsolicited email, also known as 'spam' or 'junk' emails do not: x Release a quarantined email messages unless you are confident it is a genuine business-related email. x Open attachments or click on a link in an unsolicited email. x Forward chain emails or messages where you do not recognise the sender. x Sign up to internet and email subscription lists unless it is for business purposes. x Follow unsubscribe instructions unless you have good reason to trust the source. In cases of doubt contact the ICT Service Desk for further advice.
Webmail	The use of web-based email accounts (for example: Hotmail, Gmail, iCloud, AOL etc) is permitted in accordance with the rules for personal use (see Step 9 'Follow the rules for personal use'). Webmail/private email accounts must not be used for business purposes. It is important that vigilance and professional standards are maintained when accessing webmail from Brigade computers because protection against cyber threats, such as viruses, is not assured to Brigade standards.

Step 7: Be safe online

Goals:

- Harm to the Brigade's reputation is prevented.
- Brigade computers are not exposed to harmful computer viruses.
- Brigade information is not shared inappropriately.
- Online identities are protected.
- Brigade computer facilities are not abused.
- Cloud computing is used safely.

Description	**Policies**
Web filtering	User access to the internet and to specific sites, is controlled and monitored through the use of technical controls to prevent access to certain categories of sites that the Brigade has decided as being inappropriate or may introduce unnecessary risk. Where a business requirement exists to access a website or category of website that is filtered, a request should be submitted to the ICT Service Desk. Access to normally filtered websites must only be used for the purposes authorised.
Cloud Computing and collaborating online	Internet-based 'Software-as-a-Service'[9] solutions hosted by third parties to process personal data and other Brigade information must be approved by the Brigade's chief information officer. ✓ Always follow Step 4 'Protect your identity' when using cloud services. ✓ Always be vigilant to the threat of phishing emails exploiting trust in online services, which could even be sent from the compromised account of someone you know. You must not: x Use online file transfer websites (e.g. WeSendit, WeTransfer) to transmit Brigade information. If you have a business requirement to use the Brigade's approved large file transfer facilities, contact the IT Service Desk to get started. x Use unapproved online storage websites (e.g. Google apps, Box, Dropbox) to store Brigade information. Exceptions may be approved by the chief information officer, e.g. for official collaboration purposes led by the Brigade's partners. x Upload the Brigade's sensitive information or personal data to partner-led online collaborations that are not managed by the Brigade.
Protecting the Brigade from viruses and other security incidents	You must not: x Download files from websites that offer peer-to-peer file sharing. x Access, download, print or transmit to other Brigade users or users other organisations connected to the internet, any material likely to cause offence to others (irrespective of whether you personally find any such material insulting or distasteful). x Download, duplicate or transmit tools designed to test or compromise security solutions or virus tools.

[9] 'Software as a Service' (SaaS) solutions are services deployed over the internet by third party suppliers. SaaS solutions process corporate information in an environment that is not managed by the Brigade and therefore require assessment of supplier adequacy by the ICT Department prior to evaluation and approval of the service.

Description	Policies
	x Access the internet by routes other than through the Brigade's centralised servers unless authorised by the chief information officer. x Use your Brigade email address for personal mail lists or shopping websites, etc. As a matter of good practice: ✓ Only download material from the internet if you trust the site. ✓ Only join mailing lists when there is a good business need to do so. ✓ Avoid clicking through emails unless you are confident that you trust the link. It is safer to type the website address directly into your browser, but be careful to avoid a mis-spelling which could take you to a copycat website. You can bookmark sites you use regularly. ✓ Avoid unnecessarily using websites on the internet that use http (secure website addresses begin with https, e.g. https://london-fire.gov.uk) but be aware that https (or the padlock icon) does not guarantee the site is safe.
Social Media	Access to many social networking websites is permitted for all staff through the Brigade's computing environment. For example, Facebook, Twitter, LinkedIn and Instagram. Use of social networking sites, both in and outside of work, must be in compliance with the requirements of Policy number 944 – Social media policy for the London Fire Brigade.
The Brigade's reputation and corporate identity	You must not: x Use the internet in a manner that could be harmful to the Brigade's reputation, for example, not following the rules set out in this AUP or Policy number 944 – Social media policy for the London Fire Brigade in what you say and do online, or otherwise conducting yourself in an unprofessional manner online linked to your work. x Use London Fire Brigade's corporate identity on the internet without the prior written agreement of the assistant director, communications.
Accountability	You are accountable for all internet access by your network account. Ensure you: ✓ Never share your internet access with another user. ✓ In the event you accidentally access inappropriate content you should exit the site immediately and report it to a line manager (for your own protection).
Monitoring internet usage	All internet access is monitored and logs are retained for up to six months containing the addresses of websites visited by named individuals, including denied access attempts.

Step 8: Be secure when mobile or working remotely

Goals:

- The confidentiality of information is appropriately maintained.
- Portable equipment is kept safe.
- Only authorised people can access LFB systems and information remotely.

Description	Policies
Portable equipment/working away from the office	You must keep all Brigade portable ICT equipment (e.g. laptops, tablets and phones) under your direct control at all times. Take particular care when travelling and never leave the item unattended or visible in a vehicle. In the event of equipment or a device being lost or stolen you must report it immediately to the ICT Service Desk. You may only use Brigade-issued removable media, peripheral (e.g. digital camera) and storage devices (e.g. USB devices) for the transfer and storage of Brigade information, and only when a business need to use removable media exists. You must not store Brigade data on any portable ICT equipment or device with a security classification of 'OFFICIAL'[10] or above or personal[11] or sensitive data, unless it is protected by suitable encryption. Brigade issued laptops and tablet devices are issued with disk encryption as standard. If in doubt, contact the ICT Service Desk. PINs and passwords, including encryption PINs (and any recovery code provided) protect the data stored on devices against unauthorised access. PINs, passwords and codes must not be attached to or stored with the device. All remote and mobile working must be carried out using methods approved by the Brigade.The use of your private online accounts (e.g. webmail; online storage or file sharing) for transferring the Brigade's OFFICIAL information between the Brigade's network and your privately-owned computer/storage is not permitted. Always take care not to be over-looked if you are required to work in a public place.
Remote access and security tokens	Access to the Brigade's ICT network, from a remote location (including from home), must only be through the Brigade's approved remote access facilities. When working remotely from home or other locations you must take all reasonable steps to keep the Brigade's information secure. You must use a password protected screen lock when leaving an open session unattended at home and generally use prudence to apply the same controls and safeguards that you would when at your normal place of work. Take particular care to ensure that printed personal data is managed securely and securely disposed of when no longer required. If you have been issued a security token you must: ✓ Keep it under your direct control or securely locked away at all times. ✓ Keep your password/passcode/PIN secret. ✓ Report any loss of your security token to the ICT Service Desk immediately.

[10] See footnote 7.

[11] See Brigade Policy number 351 – 'Data Protection Law' for the definition and application of 'personal data'.

Step 9: Follow the rules for personal use

Note about personal use and business use:

In this AUP, and in our application of business rules, we interpret 'personal use' as being information and activities that is of a purely personal nature or about private household activity. Information that is about, or connected to professional or Brigade activity, is business data; this is regardless of what device, system or setting that activity takes place in (e.g. using a personal email account (like Hotmail/Google) for work related activity is still business use and business data subject to legal obligations and restrictions.

Goals:

- Information is processed using approved solutions.
- Virus infections and data loss incidents through the use of unmanaged equipment and private accounts are avoided.
- Business is not disrupted by personal use of the Brigade's facilities.

Description	Policies
Personally-owned equipment and private facilities	Use Brigade approved solutions for working with the Brigade's information. You must not store any Brigade data on privately owned ICT equipment or devices unless it is already in the public domain (e.g. published on the Brigade website) or is not subject to a Brigade security classification.[12] Particular care must be taken not to store or process personal data on privately-owned equipment. If in doubt, contact the data protection officer for clarification. When you use your personal email, private WhatsApp account or other private accounts, the Brigade cannot protect you. You may also be bound to terms of use that are not compatible with business use and requirements. It is a criminal offence to knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller. x Never use a private account to store Brigade data.
When personal use is permitted	You are allowed reasonable use of the Brigade's computer facilities for personal purposes, outside official work time or station work routines, providing it is not detrimental to your own or any other employee's work performance. Be aware that the Brigade does not guarantee confidentiality for any personal use of Brigade computer facilities. Personal use includes: ✓ Preparing, and sending domestic/family correspondence. ✓ 'Public Service' activities (e.g. involvement in charities and membership of governing bodies for schools, hospitals, etc.). ✓ Communicating with trade union representatives (but see exclusions in this section below). ✓ Browsing the internet and using private email and social media sites where access is available or using a Brigade mobile phone, outside official work time or station work routines (see also Policy number 944 - Social media policy). ✓ With Brigade mobile phones: downloading apps from the Google Play Store, or Windows Store, download music and videos, store personal photos/videos, Apps may not be downloaded from unofficial app stores as

[12] See footnote 7.

Description	Policies
	these cannot be trusted and there is no way of knowing if the app is genuine. You should always exercise care when using your device. ✓ To privately advertise items for sale[13]. You must not use Brigade computer facilities for: x Any activity which is in pursuance of industrial action (see Appendix 1). x Any commercial purposes, running a business or outside employment, whether paid or unpaid. x Gambling. x Political activities. x Product advertising. The Brigade does not accept any responsibility or liability, for private transactions you conduct over the internet using its systems, where you choose to use your personal credit or debit card for internet purchases or in respect of personal transactions generally.
Separating business and personal use on your Brigade mobile phone	The Brigade uses software to manage the separation of business and personal use on Brigade mobile phones through secure containers for business applications and data (business "workspace"). This gives you some freedom to personalise the phone while providing a secure workspace for conducting Brigade business. The Brigade is not responsible for, the private data you store or process, which should be in the phone's personal space and which you do at your own risk, and the Brigade is not responsible for protecting it or any losses you may suffer through your private use. SMS communication (text) and telephone for business use happens in the personal side of your phone, but any data about this remains the property of the Brigade and is subject to all applicable freedom of information and data protection laws. If you decide to use apps on the personal side of your phone for a work related (but not essential) need (such as Workplace, Trello or Slack) you must ensure that the information is appropriate for public access and if that information was lost or compromised, it would not embarrass the Brigade, its reputation or cause harm to the Brigade's work or staff. If you wish to hold more sensitive data then you need to request (via the ICT Service Desk) that the app is made available in the business Workspace. You have access to a camera in both the business workspace and personal area of your phone. Taking photos for work purposes, which must be in accordance with the requirements of your role, must be via the camera in the business workspace. Only photos taken for personal use may be stored on the personal side of the phone. You need to be aware that if you leave the Brigade, or no longer have a business requirement for a Brigade mobile phone, your private data (including images, personal contacts, etc.) stored on the phone will be wiped and you will

[13] Facilities are available to advertise items for sale on ***Hotwire***.

Description	Policies
	no longer have access to it. Before returning your phone you should ensure you remove any personal data you require. You may not store or access the Brigade's information through the personal area of your phone or save Brigade data to your personal data area on the phone (or elsewhere).
Back-up of personal data from mobile phones to cloud storage	If you choose, you can back-up your private data from your Brigade mobile phone to cloud storage which can be restored if your phone is lost, stolen or breaks, or so you can take it with you if you leave the Brigade. You are advised to back up all your private data to a cloud storage service. For example, you can do this by setting up the phone to backup to Google Drive.

Step 10: Always report security incidents

Goals:

- Reporting security incidents enables action to be taken to avoid or minimise harm to the Brigade.
- Problems can be quickly identified and remediated.
- Incidents reported may help to identify a more serious problem.
- Lessons can be learnt from incidents that are reported to prevent recurrence.

Description	Policies
Reporting security incidents	All security incidents must be reported to the ICT Service Desk as quickly as possible: • By email: IT Service Desk (Tel. #89100) it.servicedesk@london-fire.gov.uk • By phone: extension 89100 Urgent incidents, for example a virus infection, must be brought to the attention of the ICT Service Desk immediately by phone to ensure that an appropriate response can be initiated. Even small incidents should be reported as they might aid investigation of a bigger issue.
Loss of Brigade mobile equipment	If Brigade ICT equipment (including your mobile phone) is lost or stolen you must report it to the IT Service Desk on extension 89100 immediately so that steps can be taken to protect the Brigade's data and the device. If your mobile device is lost or stolen, the Brigade will remotely wipe all data. In the case of mobile phones, only the business workspace will be wiped. If your mobile equipment is stolen you must also report it to the police and pass the crime reference number to the IT Service Desk.
Reporting security concerns	If you are concerned about a security issue or security practices, you should report it to the IT Service Desk. Such concerns raised may help to protect the Brigade through improvement. Even, if you are uncertain about something, you should still report it.
Don't be afraid to report	Even if you are worried that you might have made a mistake, it is really important that you report security concerns quickly. Prompt reporting could help ICT to minimise or contain damage. Reporting can also help to identify where improvements can be made.
Personal data breaches	If, for any reason, you believe there has been a breach of Brigade personal data (any situation where there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data; including breaches that are the result of both accidental and deliberate causes) this must be reported to the Brigade's data protection officer (dataprotectionofficer@london-fire.gov.uk or x30300) as soon as this is discovered.

4 Monitoring the use of computer facilities

4.1 Monitoring of the use of computer systems and networks, and user actions (e.g. logon/off, swipe card access to LFB buildings, telephone or printer usage, audit logs and records etc) is carried out by the Brigade, by automated and manual processes. This monitoring information may be made available to line managers in accordance with the provisions of Appendix 2 - Procedure for accessing user files/logs when the user has not given permission for access. Monitoring information will not be used for any other purposes than set out in Appendix 2, unless otherwise required by law, and will only be used by authorised persons having a valid business need to access this monitoring information.

4.2 ICT staff can remotely monitor the screens and keystrokes of individual workstations in order to help resolve problems reported via the ICT Service Desk. ICT staff will obtain a user's permission before using this remote monitoring facility and will advise them when such monitoring has ended.

4.3 Network printing may be subject to monitoring in order to identify usage contributing to unnecessarily high printing costs and corresponding environmental impact. Such reports may be made available to managers for a legitimate reason, for example, investigation of excessive print costs.

4.4 Telephone and mobile data will be monitored to assess usage of allowances and restrict excessive use of data, calls and texts on mobile phones.

5 Data protection and freedom of information law

5.1 The provisions of all applicable data protection and freedom of information law apply to all Brigade information stored and accessed through your Brigade devices, including mobile phone.

5.2 To comply with information requests, the Brigade may need to access and copy data held on your workplace computer including MS365 tools such as eDiscovery and the business area of your mobile phone.

5.3 Private and personal information held on a Brigade mobile phones, i.e. information that does not relate to your work, will not be subject to either data protection or freedom of information law providing it does not relate to work activities. Personal and private information held on, or accessed via, your Brigade mobile will not normally become Brigade information simply because it is stored on or accessed from a Brigade device.

5.4 Whilst you should not use personal email, text (SMS), social media or the personal space on the phone for business purposes, any LFB business data that is held on the personal area of the phone may need to be provided to the Brigade in order to respond to valid information requests under data protection or freedom of information law.

5.5 The Brigade reserves the right to undertake investigation on all devices, including mobile phones, in order to meet its legal obligations or to investigate suspected misuse.

Appendix 1 - Trade union use of Brigade computing facilities

The Brigade recognises the value of using computer facilities to enable communication on matters of joint interest and will use email to conduct business with senior officials of accredited trade unions. To facilitate this, the Brigade will:

- ✓ Allow staff, who are also accredited trade unions officials, to use their account for trade union purposes relating to joint industrial relations activity within the Brigade. Trade unions will be required to seek approval for officials to use computer facilities as part of the annual arrangement for notifying the Brigade of accredited representatives.
- ✓ Provide facilities (e.g. Trade Unions SharePoint site), ***hotwire*** (intranet) pages) that allow recognised trade unions to make information available to their members or seek their members' views under agreed joint consultation arrangements and to view, print or download material. A trade union's official will be permitted to use email to draw union members' attention to items posted to any electronic notice email board and to use email distribution lists for this purpose. Requests for such facilities should be made to the head of human resources and development by the most senior official of the trade unions concerned who will be the designated officer responsible for the management of the facility.

The Brigade's email system must not be used by trade union officials (or other employees) to distribute documents which are trade union's literature, newsletters, circulars, notices, minutes, agendas, etc. Such items should be posted to a facility as described above (where provided), or displayed on a traditional noticeboard or circulated using the internal post. Each item posted to an electronic notice board must :

- ✓ be approved by the appropriate senior union official;
- ✓ comply with the Brigade's policy; and
- ✓ be information about industrial relations matters connected with the Brigade and the range of services provided to union members.

Where necessary, trade unions may be responsible for providing computer hardware which is compatible with the Brigade's equipment and approved by the chief information officer.

Facilities are governed by the Brigade's trade union facilities arrangements with the recognised trade unions. Accredited trade union officials may make use of the Brigade's computer facilities for the purpose of communicating with management.

Brigade computer facilities must not be used for any activity which is in pursuance of industrial action/breach of contract. The Brigade reserves the right to block emails entering the Brigade from trade unions (or other agencies/individuals) which promote industrial action/breach of contract.

Trade unions and their accredited representatives, who are given access to computer facilities, must comply with the provisions of this AUP. The use made by trade unions and their representatives of computer facilities will be subject to the Brigade's monitoring arrangements as detailed in section 4 of the AUP.

Failure to comply with any of the above provisions may result in withdrawal of ICT facilities and, depending on the seriousness of the breach, disciplinary action.

Appendix 2 - Procedure for accessing user files/logs when the user has not given permission for access

Background

1 A request to access any user files or logs may be for normal business purposes (for example, where the user is unexpectedly away from work), or to investigate where abuse of facilities or other misconduct is reasonably suspected. Such a request might include emails or files held on personal drives, and any files temporarily stored off-line (e.g. on back-up tapes or other storage media), details of logon/off actions, swipe card access to Brigade buildings, telephone and printer records, audit logs, etc). Access includes the download of log data.

2 Any person granted access to another user's computer emails/files/logs will be subject to data protection law.

Circumstances when access will be granted

3 Access to a user's computer files/logs will only be given in the following circumstances:

(a) Where abuse of facilities or other misconduct is reasonably suspected.

(b) Immediate access is required for operational or legal reasons.

(c) In other circumstances where, in the opinion of the head of department concerned and with the agreement of the chief information officer (CIO) or data protection officer (DPO), that such access is necessary for efficient discharge of the Brigade's business, to safeguard the security of computer systems, etc.

4 Access to user accounts, emails or logs may also be granted where there is reasonable suspicion of some misuse or other misconduct, but where investigation is needed to trace the actions to a named individual. Requests must be to access specific files of a named user(s). Requests made for continuous access to the files or emails of a named user will not be agreed; requests must be specific and for a specified period of time.

Arrangements for access

5 A request for access should be made by a head of service or a member of the Top Management Group who must satisfy themselves that the request is valid and proportionate. The request then goes to the CIO or the Brigade's DPO who can approve and action the request. In the absence of the CIO/DPO their nominated deputy may approve such a request.

6 The CIO/DPO will need to be satisfied that any request is properly authorised and falls within the circumstances listed in paragraph 3 above. In cases of doubt, the matter may be referred to the director of corporate services for decision.

7 If a request for access is agreed, the CIO/DPO will authorise a named officer in ICT Department to liaise with the head of department to access the material requested. Because personal data may be available; access to requested data (particularly mailboxes) will normally be granted to a member of ICT staff and department access to material will be supervised by that member of ICT staff. The CIO/DPO will state specifically the extent and/or restrictions applied to any search or access in writing.

Notification to the user (author) of files accessed

8 If access is for operational/legal reasons and the user is away from work, the head of service should take steps to ensure that the user is notified of the request for access (and why) when the user returns to work.

Proper audit trail

9 The head of department and the head of ICT will maintain proper records to ensure the implementation of the procedure set out in this appendix can be monitored.

Document History

Assessments

An equality, sustainability or health, safety and welfare impact assessment and/or a risk assessment was last completed on:

EIA	30/06/20	SDIA	L - 11/05/20	HSWIA	11/05/20	RA	N/A

Audit trail

Listed below is a brief audit trail, detailing amendments made to this policy/procedure.

Page/para nos.	Brief description of change	Date
Page 4	Reference to cancelled PN346 replaced with reference to PN973 – togetherness policy.	28/01/2022
Page 18	Paragraph 5.2 updated to include MS365 tools such as eDiscovery.	03/02/2023
Throughout	Reference to cancelled PN973 – togetherness policy replaced with Brigade's Culture Review.	10/04/2024
Page 4	Reference to cancelled PN0340 replaced with a link to copyright information on hotwire.	10/02/2026

Subject list

You can find this policy under the following subjects.

Information Technology	Workplace regulations

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

Considered by: (responsible work team)	**FOIA exemption**	**Security marking classification**