IT Acceptable Use Policy

BIRMINGHAM
2022
commonwealth
games

January 2020

Document Control

Document Information

Document title:	IT Acceptable Use Policy
Document author:	Head of IT Services Delivery
Document reference number:	CPOL-TEC-003
Date reviewed by Senior Management Team:	10th March 2020
Date approved by OC Board:	Not applicable
Date and outcome of Equality Impact Assessment:	9th January 2020 – No impact on protected characteristics
Date document issued:	13th March 2020
Review date, if applicable:	Not applicable
Target audience (e.g. all staff):	All users of Birmingham 2022 IT and telecommunications services
Subject area (e.g. Finance, HR, Legal):	Technology

Version History

Version No	Lead	Date change implemented	Reason for change
V0.1	Technology	09/01/2020	Updated with OC policy template

Consultation History

Position	Organisation
Chief Information Officer	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Chief Legal Officer	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Head of Human Resources	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Compliance Manager	Birmingham Organising Committee for the 2022 Commonwealth Games Limited

Disclaimer

This is a proprietary Birmingham Organising Committee for the 2022 Commonwealth Games Limited (Birmingham 2022) document and is not to be relied upon by any person other than Birmingham 2022 and its staff and those who are expressly authorised in writing to rely on the contents of this document. Birmingham 2022 makes no express or implied guarantees, representations or warranties to any third party as to whether the requirements of this document will be fulfilled by Birmingham 2022, its staff, agents, contractors, authorised representatives or anyone else to whom the document relates or refers. Birmingham 2022 accepts no liability for any reliance by any third party on the contents of or the procedures detailed in this document.

Copyright

Contents

1. Purpose

This IT Acceptable Use Policy provides a framework for the use of Birmingham 2022's IT facilities and covers the responsibilities and required behaviour expected of users of those facilities.

It is aimed to minimise security risks and ensure the use of IT facilities is carried out in compliance with all applicable laws and regulators' guidance and policy documents.

It also gives important information about our rules on the use of IT facilities, how we monitor the use of those systems, rights and obligations in relation to data protection and the consequences of failure to comply with this policy.

This policy applies to all information systems, in whatever form, relating to Birmingham 2022's business activities, and to all information systems accessed by Birmingham 2022 relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Birmingham 2022 or on its behalf.

2. Scope

This policy applies to all Birmingham 2022 employees, volunteers and contractors (including contract staff, consultants, secondees and temporary and agency personnel) (hereafter referred to as 'individuals').

The policy covers:

- Access to all Birmingham 2022's IT facilities, wherever they are located and however they are accessed. This includes but is not limited to individuals working in Birmingham 2022's Corporate Headquarters, and those working remotely at Games venues, whilst travelling, in their homes or in hotels.
- IT and information communications facilities are defined as any of Birmingham 2022's IT resources, including networks and access to the internet, email, computers, telephony equipment, laptops, other mobile devices, and any other related software and hardware. Individuals using personally owned equipment, including personal mobile devices attached to Birmingham 2022's network are also bound by this policy. This policy should be interpreted as having the widest application as to include new and developing technologies and uses, which may not be explicitly referred to.

3. Objectives

The objective is to ensure that all individuals can understand their responsibilities when using/accessing Birmingham 2022 technology equipment, IT systems (including email) and the internet.

4. Responsibilities

4.1. Executive Management Team

- The Executive Management Team have overall responsibility for ensuring their teams comply with this policy.

- The Head of IT Services Delivery has overall day to day responsibility for information security within the organisation.
- If the working practices of their team conflict with this policy, Executive Managers are responsible for raising any issues with the Head of IT Services Delivery.

4.2. Line Managers

- Line Managers at all levels of the organisation are responsible for ensuring those reporting to them understand and comply with this policy;
- Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data; and
- Line Managers should Review and provide approval in support of any exceptions to the policy.

4.3. All individuals

All individuals have personal responsibility for ensuring that they read and comply with this policy and with any directions related to this policy received from Line Managers.

5. Acceptable Use Policy

5.1. Computer access control – individuals' responsibilities

Access to Birmingham 2022's IT systems is controlled by the use of user IDs, passwords and/or tokens. All user IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are personally accountable for their actions on Birmingham 2022's IT systems.

Individuals must not:

- Disclose their credentials or allow anyone else to use their user ID/token and password on any Birmingham 2022 IT system;
- Use someone else's user ID and password to access Birmingham 2022 IT systems;
- Leave their password unprotected (for example writing it down and not keeping the document safely);
- Leave their user accounts logged in at an unattended and unlocked computer;
- Perform any unauthorised changes to Birmingham 2022's IT systems or information;
- Attempt to access data that they are not authorised to use or access;
- Maintain a log in status connected to the internal network during non-working hours;
- Exceed the limits of their authorisation or specific business need to interrogate the system or data;
- Connect any non-Birmingham 2022 unauthorised device to the Birmingham 2022 network or IT systems, without specific authorisation from the Technology Service Desk, or as otherwise agreed by an individual's line manager or the HR team;
- Store Birmingham 2022's data on any unauthorised Birmingham 2022 equipment or personal device;

- Other than for legitimate business purposes, within the agreed data sharing agreements and using appropriate means to protect the data – (e.g. Birmingham 2022 extranet), give or transfer Birmingham 2022 data or software to any person or organisation outside Birmingham 2022.If in doubt please seek clarification from your Line Manager.

5.2. Internet and email conditions of use

Birmingham 2022’s internet and email is intended for business use only. Personal use is permitted where such use:

- does not affect the individual’s work performance;
- is not detrimental to Birmingham 2022 in any way;
- does not breach any term and condition of employment;
- does not place the individual or Birmingham 2022 in breach of statutory or other legal obligations;
- does not damage the reputation of Birmingham 2022; and
- does not embarrass or compromise Birmingham 2022 any way.

We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- use the internet or email to facilitate harassment, bullying and/or victimisation of a member of Birmingham 2022 or a third party;
- use the internet or email to promote discrimination on the basis of race, gender, gender reassignment, pregnancy or childbirth, religion or belief, disability, age or sexual orientation;
- access inappropriate content when using Birmingham 2022 IT facilities and not intentionally visit sites that are obscene, indecent or promote illegal activity;
- use profanity, obscenities, or derogatory remarks in communications;
- access, download, send or receive any data (including images), which Birmingham 2022 considers offensive in any way, including material which is sexually explicit, discriminatory, defamatory, libellous, extremist or which has the potential to radicalise themselves or others;
- use the internet or email to make personal gains or conduct a personal business;
- use the internet or email to gamble;
- use the internet or email with the intent to defraud or deceive a third party;
- use the internet or email to advocate or promote any dishonest or unlawful act;
- use the internet or email to carry out any hacking activities;
- use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam;
- place any information on the Internet (including Social Media) that relates to Birmingham 2022 or any individuals anyhow related to Birmingham 2022, alter any information about it, or express any opinion about Birmingham 2022 or any individuals anyhow related to

Birmingham 2022, unless they are specifically authorised to do this (please refer to the Social Media Policy and Guidelines for further information);

- send externally any unprotected information that is considered official, sensitive, confidential, secret, top secret or that contains personal data;
- forward Birmingham 2022 mail to personal (non-Birmingham 2022) email accounts (for example a personal Hotmail account);
- make official commitments through the internet or email on behalf of Birmingham 2022 unless authorised to do so;
- download copyrighted material such as music media (MP3) files, pictures, film and video files (not an exhaustive list) without approval from the Technology Service Desk;
- in any way infringe any copyright, database rights, trademarks, intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party;
- download any software from the internet without prior approval of the IT Services Functional Area;
- wilfully or recklessly damage any Birmingham 2022 IT facilities.

5.3. Clear desk and clear screen policy

In order to reduce the risk of unauthorised access or loss of information, Birmingham 2022 enforces a clear desk and screen policy as follows:

- personal data and any other business information must be protected using security features provided for example secure print on printers and privacy screens;
- computers must be logged off/locked (for example with a Kensington lock) or protected with a screen locking mechanism controlled by a password when unattended;
- care must be taken to not leave confidential, business related material or documents containing sensitive information or personal data on printers or photocopiers;
- all business-related printed matter must be disposed of using confidential waste bins or shredders;
- all individuals must adhere to the B2022 clear desk policy (in the Office Guide).

5.4. Working off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with the Birmingham 2022's Remote Working Policy and the confidentiality provisions for remote working detailed in the Confidentiality and Data Protection Policy;
- Equipment, printed materials and media (for example, USB stick) taken off-site must not be left unattended in public places and not left in sight in a car;
- Laptops must be carried/treated as hand luggage when travelling;
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used;
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

5.5. Mobile storage devices

Media devices (such as memory sticks and removable hard drives) must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Birmingham 2022 authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data. Data should not be stored on mobile storage devices for longer than is required and should be completely and securely deleted when it is no longer required. Users must not transfer B2022 data from an encrypted mobile media device to an unencrypted mobile storage device.

5.6. Audio visual equipment

Audio visual equipment (such as televisions, laptops, microphones & speakers) must only be used for legitimate business purposes.

Individuals must not:

- play copyrighted material such as music media (MP3) files, pictures, film and video files (not an exhaustive list) without appropriate approval.
- use equipment for the playback of inappropriate content which Birmingham 2022 considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- watch live terrestrial broadcasts (via aerial, satellite or applications such as BBC iPlayer) in B2022 venues where no TV license has been obtained.
- re-configure equipment or download applications (such as IPTV or VPNs) for the purposes of avoiding national or regional broadcasting rights.

5.7. Reprographic devices

Reprographic devices (such as printers, scanners and copiers) must only be used for legitimate business purposes.

Before printing any documents or diagrams, individuals should consider carefully if hardcopies are required. Wherever possible, projectors or screens should be used to display documents or diagrams. If printed materials are required, individuals must consider what is printed and who could view it when printing, when travelling between meetings or venues, and when working at a desk.

All B2022 documents must be disposed of in the confidential waste bins available throughout the B2022 offices and venues.

5.8. Software

Individuals must use only software that is authorised by Birmingham 2022 on Birmingham 2022 computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Birmingham 2022 computers must be approved and installed by the Birmingham 2022 IT Services department: typically made available through the Company Portal.

Individuals must not:

- Store any files (business or personal) directly on a laptop/PC (OneDrive and SharePoint should be used);
- Store personal files such as music, video, photographs or games on Birmingham 2022 IT equipment other than as otherwise approved through Birmingham 2022 (e.g. photography competition)

5.9. Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within Birmingham 2022. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- remove or disable anti-virus software;
- attempt to remove virus-infected files or clean up an infection, other than by the use of approved Birmingham 2022 anti-virus software and procedures. If in any doubt, please refer to the Technology Service Desk; or
- intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

5.10. Telephony (voice) equipment conditions of use

Use of Birmingham 2022's telephony equipment (e.g. mobile, desk or conference 'phones) is intended for business use however, individuals may make reasonable personal use of these facilities, with Line Management permission, if required.

Individuals must not:

- use Birmingham 2022 voice equipment for sending private communications on personal matters without their line manager's consent;
- make hoax or threatening calls to internal or external destinations;
- accept reverse charge calls from domestic or International operators, unless it is for business use; or
- make international phone calls where alternative methods of voice communication are available (e.g. Microsoft Teams).

5.11. Actions upon Contract Completion

All Individuals must return all Birmingham 2022 equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, to Birmingham 2022 upon termination of contract.

All Birmingham 2022 data or intellectual property developed or gained during the period of employment remains the property of Birmingham 2022 and must not be retained beyond termination or reused for any other purpose.

5.12. Monitoring and Filtering

Birmingham 2022 has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

All data that is created and stored on Birmingham 2022 computers is the property of Birmingham 2022, however wherever possible Birmingham 2022 will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will commence where reasonable suspicion exists of a fraudulent behaviour, misconduct, breach of this or other related IT and Confidentiality policies, in line with the Staff Privacy Notice (sent to all new employees). Email monitoring may also take place exceptionally in the case of long-term absence, subject to the controls below.

Any monitoring will be carried out in accordance with audited, controlled internal processes in accordance with the procedure set out in Appendix 1 which requires a formal request to launch an investigation to be approved by the Head of HR and Chief Legal Officer. In addition, all and any monitoring will be carried out in accordance with the Data Protection Legislation (including the Data Protection Act (DPA) 2018 and General Data Protection Regulations (GDPR)), the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

6. Breaches of this Policy

Any employee who breaches this policy, knowingly or recklessly uses IT facilities for purposes other than those for which they are intended, or deliberately acts outside of their recognised responsibilities will be subject to Birmingham 2022’s disciplinary procedures, which could result in:

- An individual’s right to use the Birmingham 2022 network or IT facilities being restricted or terminated;
- withdrawal or removal of any material uploaded by that individual in contravention of this Policy; or

dismissal for misconduct or gross misconduct, and possible legal action liable to prosecution. Birmingham 2022 may terminate its relationship with other Individuals and organisations working on its behalf if they breach this policy.

7. Ongoing Review

This policy will be subject to review annually after its date of approval.

Earlier review may be required if any of the following occur:

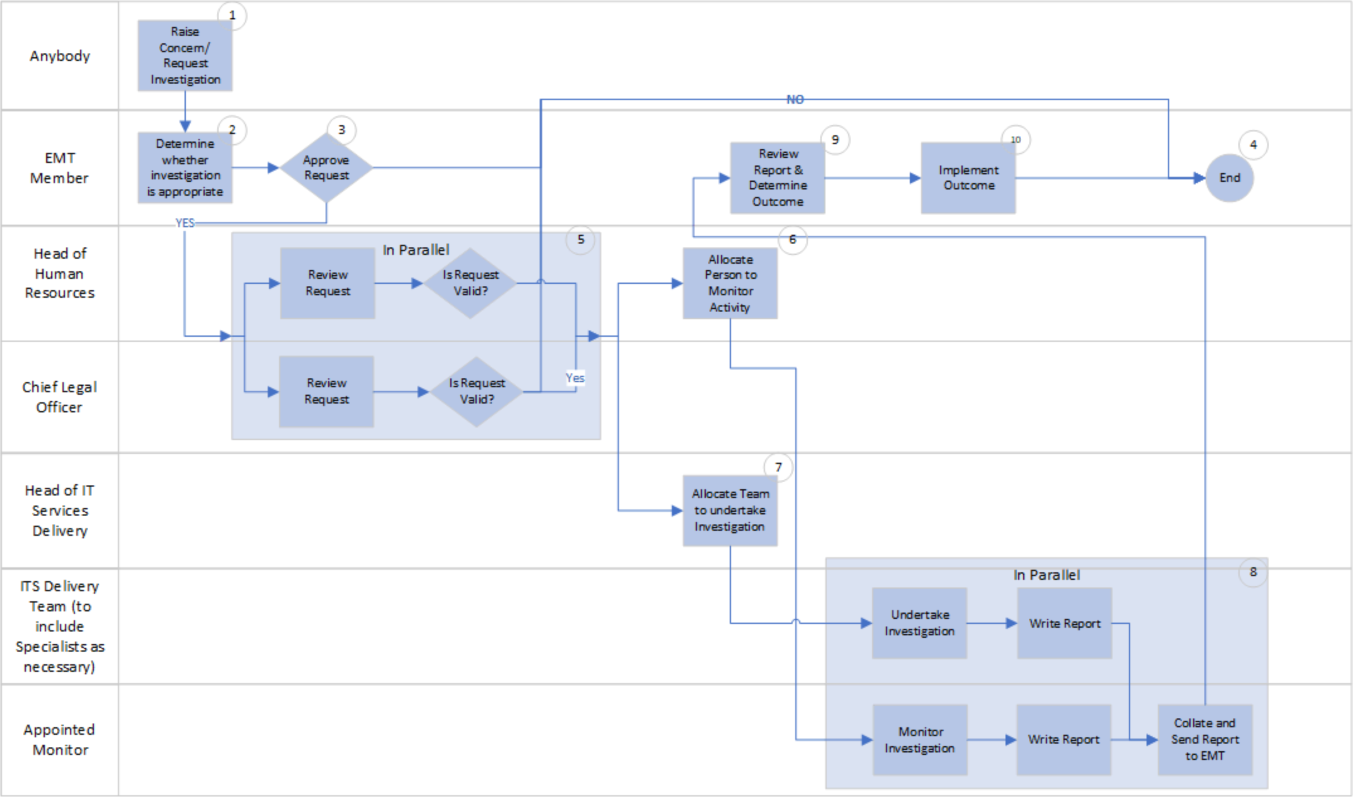
- The adoption of the policy highlights any errors or omissions in its content;
- Following monitoring of complaints made by individuals via the internal review process, amendments are required to the content of the policy;
- Where relevant changes in legislation or national guidance impact upon the content of this policy.

8. References

8.1. Related References

- The Data Protection Act (DPA) 2018 (http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
- The General Data Protection Regulation (EU) 2016/679
- Regulation of Investigatory Powers Act 2000 (http://www.legislation.gov.uk/ukpga/2000/23/contents)
- The Computer Misuse Act 1990: www.legislation.gov.uk/ukpga/1990/18/contentsCommunication Act 2003 (http://www.legislation.gov.uk/ukpga/2003/21/contents)
- The Human Rights Act 1998
- The Equality Act 2010
- General Data Protection Regulations legislation guidance (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/)
- Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 (https://www.legislation.gov.uk/uksi/2000/2699/contents/made)
- The Employment Practices Code, Information Commissioner's Office (https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf)
- Disciplinary Action Policy (https://birmingham2022.sharepoint.com/all-staff-information/Documents/B2022%20Policies/HRO.003%20B2022%20Disciplinary%20Action%20Policy.pdf#search=disciplinary%20action)
- Confidentiality and Data Protection Policy (https://birmingham2022.sharepoint.com/all-staff-information/Documents/B2022%20Policies/LGL.005%20B2022%20Confidentiality%20and%20Data%20Protection%20Policy.pdf#search=confidentiality%20and%20data)
- Information Security Policy (https://birmingham2022.sharepoint.com/all-staff-information/Documents/B2022%20Policies/TEC.002%20B2022%20Information%20Security%20Policy.pdf#search=information%20security)
- Mobile Device Policy (BYOD) (https://birmingham2022.sharepoint.com/:w:/r/all-staff-information/_layouts/15/Doc.aspx?sourcedoc=%7BB4DDA46E-3526-4C12-A9E6-4E826C80DA91%7D&file=DRAFT%20TEC.001%20B2022%20Mobile%20Device%20Policy%20(BYOD).docx&action=default&mobileredirect=true)
- Office Guide (Clear Desk Policy) (https://birmingham2022.sharepoint.com/all-staff-information/Documents/Office%20and%20Facilities/New%20Branding%20-%20Office%20Guide.pdf#search=office%20guide)
- Remote Working Policy [link to be added]
- Social Media Policy and Guidelines

Appendix 1 – Process Flow



Anybody
EMT Member
Head of Human Resources
Chief Legal Officer
Head of IT Services Delivery
ITS Delivery Team (to include Specialists as necessary)
Appointed Monitor
1
Raise Concern/ Request Investigation
2
Determine whether investigation is appropriate
3
Approve Request
YES
NO
In Parallel
5
Review Request
Is Request Valid?
Review Request
Is Request Valid?
Yes
9
Review Report & Determine Outcome
10
Implement Outcome
4
End
6
Allocate Person to Monitor Activity
7
Allocate Team to undertake Investigation
In Parallel
8
Undertake Investigation
Write Report
Monitor Investigation
Write Report
Collate and Send Report to EMT

Figure 1: End to end investigation process from initiation

Process Steps

ID	Who?	What?	Description
1	Anybody	Raise Concern/Request Investigation	If anybody believes they have a valid reason for an investigation to take place, this should be formally raised with a member of the EMT, either directly or through a colleague. The detail of the concern can be written (in any format), however they must be transcribed onto the form provided below at Appendix 2 (a template is provided below). The mechanism for raising a concern, as described above allows for a concern to be raised about a member of the EMT, as the request can be raised with another EMT member.
2	EMT Member	Determine whether investigation is appropriate,	The EMT Member will review the details provided on the form and determine whether this warrants further investigation, in line with the Disciplinary Action Policy (see above).

ID	Who?	What?	Description
3	EMT Member	Approve Request	If the EMT member believes that the request is appropriate, then they will sign the form and pass to both the Head of Human Resources and the Chief Legal Officer for further consideration. However, if they believe that the request is not appropriate, the form should be updated to reflect this, and the process ends here.
4	EMT Member	End	The form will be returned to the appropriate EMT member who will update the form and end the process.
5	Head of Human Resources Chief Legal officer	Review Request	The Head of Human Resources will review the request to determine whether further investigation is required. If they believe that the request is appropriate, then they will sign the form. The Chief Legal Officer will review the request to determine whether further investigation is required. If they believe that the request is appropriate, then they will sign the form. If both sign the form, then the form will be passed to the Head of Human Resource and Head of IT Services Delivery to allocate resources. If one, or both of the Head of HR or Chief Legal Officer do not believe that further investigation is justified, then the form will be updated, and the process will end here.
6	Head of Human Resources	Allocate Person to monitor process	The Head of Human Resources will allocate an individual to work with the IT Services Delivery team to monitor the investigation to ensure that the investigation team are following an appropriate process. They will raise any concerns with the Head of Human Resources.
7	Head of IT Services Delivery	Allocate team to undertake investigation	The Head of IT Services Delivery will allocate an individual or team (with appropriate specialist knowledge and access) to investigate the incident as reported.

ID	Who?	What?	Description
8	IT Delivery Team	Undertake Investigation	The IT Delivery Team will undertake the investigation to determine whether there is anything in breach of this (or other policies).
		Write Report	They will note and summarise their findings in a report.
		Monitor Investigation	The Appointed Monitor will monitor the investigation to ensure that the investigation team are following an appropriate process.
	Appointed Monitor	Monitor Activity & Raise Concerns	They will raise any concerns with the Head of Human Resources or the Data Protection Office (as appropriate).
		Write Report	They will note and summarise their findings in a report.
		Collate Report	They will collate input from all involved and then pass to the EMT member to determine what happens next.
9	EMT Member	Review Report and Determine Outcome	In line with the Disciplinary Action Policy (referenced above) and in conjunction with the Head of Human Resources and the Chief Legal Officer, the EMT member will review the report and determine the next steps for the individual(s) under investigation. The form will be updated with details of the review and the agreed outcome.
10	EMT Member	Implement Outcome	In line with the Disciplinary Action Policy (referenced above) and in conjunction with the Head of Human Resources and the Chief Legal Officer, the EMT Member will ensure that the agreed outcome is implemented appropriately. The form will be updated with any details of implementing the outcome. The process will end

Appendix 2 - Acceptable Use Investigation Request Form

Appendix 2

Acceptable Use investigation request

Person Requesting investigation	
Service / work area	
Date	
Nature of concern or reason for investigation	
EMT Member (name and signature)	
Approve investigation?	□
Date	
Chief Legal Officer (name and signature)	
Approve investigation?	□
Date	
Head of Human Resources (name and signature)	
Approve investigation?	□
Date	
Name(s) and role(s) of IT Services Delivery Team members assigned to investigation	
Name(s) and role(s) of HR Monitor(s) assigned to investigation	
IT Services Delivery Team members investigation report. Please provide summary here and attach a document if necessary.	

IT Services Delivery Team members investigation report. Please provide summary here and attach a document if necessary.	
EMT report review (name(s) and signature(s))	
Is review complete?	☐
Further action necessary? Please note location of additional action details.	☐
Date	

Head of Human Resources to save one copy of this document**.**