IT Acceptable Use Policy

Festival 2022 Ltd

March 2021

DOCUMENT CONTROL

Document Information

Document Title:	IT Acceptable Use Policy
Executive Owner:	Iain Reid, Chief Executive Officer
Approved By:	Festival 2022 Ltd Board
Date Approved:	5 March 2021
Review Date:	March 2022
EqIA Date:	14 April 2021

Version History

Version	Date Released	Originator	Authorised	Comments
1.0	February 2021	Adil Hussain	n/a	Policy drafted
1.1	February 2021	-	EMT	Policy approved
1.2	March 2021	-	Festival Board	Approved

Distribution List

Name	Organisation	Position
Dame Vikki Heywood CBE	Festival 2022 Ltd	Non-Executive Chair of Festival Board
Ian Reid	Festival 2022 Ltd / Organising Committee	Chief Executive Officer
David Grady	Festival 2022 Ltd / Organising Committee	Chief Financial Officer
Caroline McGrory	Festival 2022 Ltd / Organising Committee	Chief Legal Officer
Martin Green	Festival 2022 Ltd / Organising Committee	Chief Creative Officer
Phil Batty	Festival 2022 Ltd / Organising Committee	Executive Director
John Darnbrook	Festival 2022 Ltd	Head of Business Integration
Lucy Bailey	Festival 2022 Ltd	Senior Legal Counsel
Andy Peacock	Organising Committee	Senior Enterprise Architect

Disclaimer

This is a proprietary Festival 2022 Limited (the "Company") document and is not to be relied upon by any person other than the Company and its staff and those who are expressly authorised in writing to rely on the contents of this document. Festival 2022 Ltd 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 the Company, its staff, agents, contractors, authorised representatives or anyone else to whom the document relates or refers. Festival 2022 Ltd accepts no liability for any reliance by any third party on the contents of or the procedures detailed in this document.

OC Group

Festival 2022 Ltd is a wholly owned subsidiary of the Birmingham Organising Committee for the 2022 Commonwealth Games Ltd (the "OC") and is responsible for the delivery of UNBOXED (the "programme). References to the OC Group refer to company group of both Festival 2022 Ltd and the OC.

Contents

1 Purpose

This IT Acceptable Use Policy provides a framework for the use of Festival 2022 Ltd'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 Festival 2022 Ltd's business activities, and to all information systems accessed by the Company relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Festival 2022 Ltd or on its behalf.

2 Scope

This policy applies to all Festival 2022 Ltd 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 Festival 2022 Ltd's IT facilities, wherever they are located and however they are accessed. This includes but is not limited to individuals working in Festival 2022 Ltd's Corporate Headquarters, and those working remotely at UNBOXED venues, whilst travelling, in their homes or in hotels.
- IT and information communications facilities are defined as any of Festival 2022 Ltd's IT resources, including networks and access to the internet, email, computers, telephony equipment, laptops, other mobile devices, and any other related software or hardware. Individuals using personally owned equipment, including personal mobile devices attached to the Company'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 Festival 2022 Ltd technology equipment, IT systems (including email) and the internet, and to reduce operational, business and legal risk.

4. Definitions

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
- 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 Festival 2022 Ltd'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 the Company's IT systems.

Individuals must not:

- Disclose their credentials or allow anyone else to use their user ID/token and password on any Festival 2022 Ltd IT system
- Use someone else's user ID and password to access Festival 2022 Ltd 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 Festival 2022 Ltd'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 authorised or specific business need to interrogate the system or data
- Connect any non-Festival 2022 Ltd authorised device to the Festival 2022 Ltd 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 Festival 2022 Ltd's data on any unauthorised Company 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. Festival 2022 Ltd extranet), give or transfer Company data or software to any person or organisation outside Festival 2022 Ltd. If in doubt, please seek clarification from your Line Manager.

5.2 Internet and email conditions of use

Festival 2022 Ltd's internet and email are intended for business use only. Personal use is permitted where such use:

- Does not affect the individual's work performance
- Is not detrimental to Festival 2022 Ltd in any way
- Does not breach any term and condition of employment
- Does not place the individual or Festival 2022 Ltd in breach of statutory or other legal obligations
- Does not damage the reputation of Festival 2022 Ltd
- Does not embarrass or compromise Festival 2022 Ltd any way

We reserve the right, at our absolute discretion, to withdraw this privilege at any time and/or to restrict access to 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 Festival 2022 Ltd 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 Festival 2022 Ltd 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 Festival 2022 Ltd 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 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 Festival 2022 Ltd and/or UNBOXED or any individuals anyhow related to Festival 2022 Ltd and/or UNBOXED, alter any information about it or express any opinion about Festival 2022 Ltd and/or UNBOXED or any individuals anyhow related to Festival 2022 Ltd, and/or UNBOXED, 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 Festival 2022 Ltd and/or UNBOXED mail to personal (non-Festival 2022 Ltd/UNBOXED) email accounts (for example a personal Hotmail account)
- Make official commitments through the internet or email on behalf of Festival 2022 Ltd and/or UNBOXED 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 Festival 2022 Ltd IT facilities

5.3 Clear desk and clear screen policy

In order to reduce the risk of unauthorised access or loss of information, Festival 2022 Ltd 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 Festival 2022 Ltd 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 Festival 2022 Ltd's Remote Working Policy and the confidentiality provisions from 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 Festival 2022 Ltd 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 Festival 2022 Ltd and/or UNBOXED 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 and 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 Festival 2022 Ltd 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 Festival 2022 Ltd venues where no TV licence has been obtained
- Reconfigure 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 (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 where working at a desk.

All Festival 2022 Ltd documents must be disposed of in the confidential waste bins available throughout the Festival 2022 Ltd offices and venues.

5.8 Software

Individuals must use only software authorised by Festival 2022 Ltd on Company computers. Authorised software must be used in accordance with the software suppliers licensing agreements. All software on Festival 2022 Ltd computers must be approved and installed by the Festival 2022 Ltd 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, games on Festival 2022 Ltd IT equipment other than as otherwise approved through the Company (e.g. photography competition)

5.9 Viruses

The IT Department has implemented centralised, automated virus detection and virus software updates within Festival 2022 Ltd. All PC's 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 Festival 2022 Ltd anti-virus software and procedures. If in any doubt, please refer to the Technology Service Desk
- 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 Festival 2022 Ltd'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 Festival 2022 Ltd voice equipment for sending private communications on personal matters without their line mangers 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
- 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 Festival 2022 Ltd equipment and data, for example laptops and mobile devices including telephones, smartphones, USB devices and CDs/DVDs, to the Company upon termination of contract.

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

5.12 Monitoring and Filtering

Festival 2022 Ltd 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 Festival 2022 Ltd computers is the property of Festival 2022 Ltd, however wherever possible the Company 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 or 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 Festival 2022 Ltd's disciplinary procedures which could result in:

- An individual's right to use the Festival 2022 Ltd network or IT facilities being restricted or terminated
- Withdrawal or removal or any material updated by that individual in contravention of this Policy or dismissal for misconduct or gross misconduct, and possible legal action liable to prosecution. Festival 2022 Ltd may terminate its relationship with other individuals and organisations working on its behalf if they breach 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/fororganisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-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/fororganisations/documents/1064/the_employment_practices_code.pdf)

Appendix 1 – Process Flow

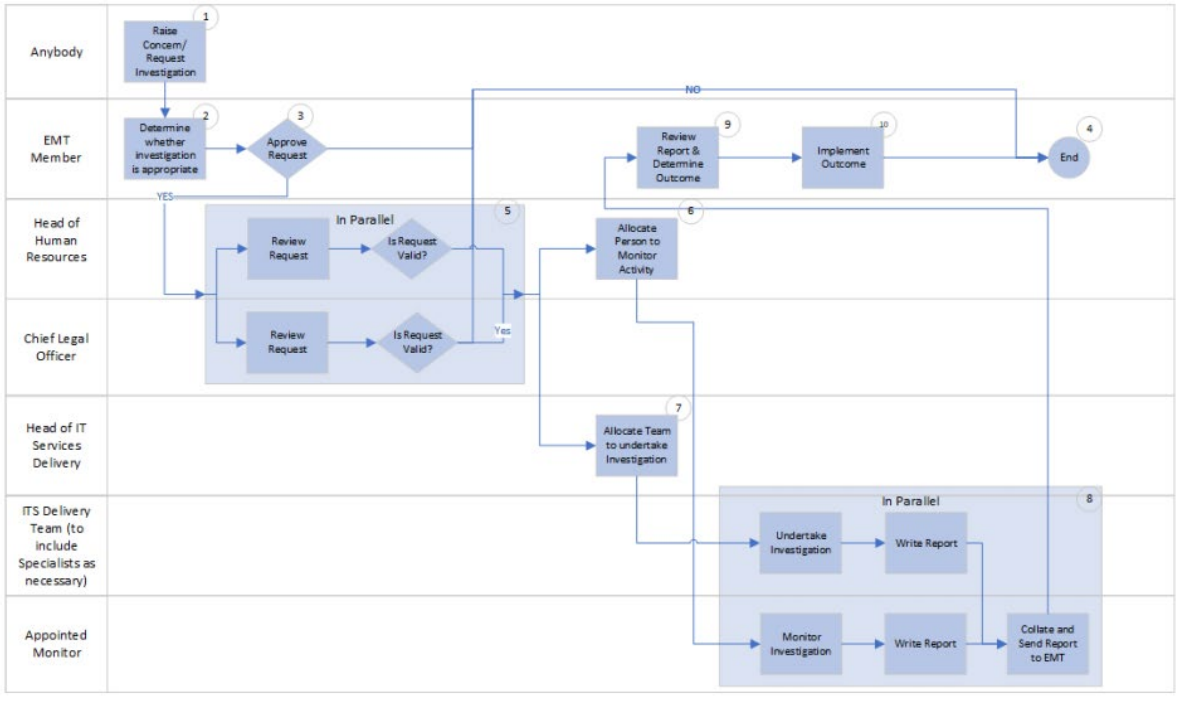

Figure 1: End to end investigation process from initiation

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).
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 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.
8	IT Delivery Team	Undertake Investigation Write Report	The IT Delivery Team will undertake the investigation to determine whether there is anything in breach of this (or other policies).

	Appointed Monitor	Monitor Investigation Monitor Activity & Raise Concerns Write Report Collate Report	They will note and summarise their findings in a report. The Appointed Monitor will 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 or the Data Protection Officer (as appropriate). They will note and summarise their findings in a 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

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.