# Acceptable Use Policy

Richard Huish Trust

| | |
|---|---|
| **Policy owner** | Director of IT and Facilities |
| **Approving board/ committee** | Trust Board |
| **Date approved** | 16/07/2025 |
| **Date implemented** | 16/07/2025 |
| **Review period** | Annually |
| **Next review due** | Summer 2026 |

# Contents



## Appendices

# 1. Introduction

**Richard Huish Trust (Huish)** is committed to ensuring that all staff / governors / visitors (guests) / students / pupils that use Huish IT devices or Huish IT systems have read and agreed the Acceptable Use Policy or summary versions where applicable. For Example. Visitor Wi-Fi acceptable use policy, KS1/KS2 AUA for Pupils and parents/carers.

### Aims

1.1 To ensure security of Richard Huish Trust (Huish) IT Systems.

1.2 To safeguard the Huish reputation.

1.3 To inform all users (staff, students, governors, and guests) of all relevant legislation relating to IT.

1.4 To provide appropriate teaching and learning environments for all Huish IT Users.

1.5 To safeguard and protect users of Huish IT Systems.

1.6 To ensure all users of Huish IT Systems are aware of the Terms and Conditions laid down by JISC (Joint Information Systems Committee).

# 2. General Computer Usage

2.1 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.

2.2 You are not permitted to download/import/install any application/program to a Huish device which has not previously been approved of by the IT Services team. Attempting such actions may lead to disciplinary action.

2.3 You are not permitted to play computer games both run locally or from the Internet, unless given permission from a member of staff. Attempting such actions may lead to disciplinary action.

2.4 There shall be no expectation of privacy when using Huish owned devices and services. Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any Huish owned devices and services.

# 3. Passwords

3.1 Huish follows best practice from the National Cyber Security Centre (NCSC) guidance.

3.2 You are responsible for safeguarding your network or email accounts and associated passwords. Never allow anyone else to know your password or allow them to use your accounts at any time. User password rights given to users should not give rise to an expectation of privacy.

3.3 For reasons of security, when changing your password for any IT system you **must** follow the guidance below.

- Do not choose obvious passwords, such as those based on easily discoverable information like the name of a pet or family member.
- Do not use common passwords such as, password, password1, p@55w0rd.
- Do not use the same password anywhere else, such as personal accounts like social media accounts or online shopping.
- Your password must not be printed, written down, or given to others.
- Do not using a similar password to a previous one e.g. adding a ! or number on the end.
- Do not use simple sequences such as 123 or abc.
- Try to use either completely random characters or long word phrases such as jydi834CSi0 or orangelikeshopping.
- Use a minimum of 12 characters.

# 4. Monitoring and Interception of Data

4.1 Huish reserves the right to monitor the usage of all Huish IT facilities in order to:

- ensure the security of its systems and compliance to this policy.
- safeguard those systems from virus/ransomware infection and spam invasion.
- monitor and prevent access to inappropriate internet sites in order to provide as secure an environment for users as possible.
- ensure compliance with the JANET (Joint Academic Network) AUP and Security Policies.

4.2 Huish telephone and computer equipment, applications and services, email and the Internet are provided primarily for work related purposes. No users may use Huish telephone equipment for personal external calls without prior approval from a member of staff, unless contacting the emergency services.

4.3 Huish has the right to monitor any and all aspects of its telephone and computer systems and networks that are made available to users and to monitor, intercept and/or record any communications made by users, including but not just restricted to telephones, e-mail or Internet communications. This also includes decrypting and inspecting HTTPS data. To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, users expressly consent to Huish doing so by agreeing to this policy. In addition, it should be noted that every time a user logs on they are agreeing to this policy.

4.4 Computer and telephone networks and user's network and e-mail accounts are the property of Huish and are designed to assist in the performance of authorised users' work. Users should, therefore, have no expectation of privacy in any communication sent or received, whether it is of a business or personal nature. The IT Services department ensures the automatic monitoring of web and email traffic is working correctly and efficiently. Manual checking of quarantined email and logs is carried out by authorised staff.

4.5 It is an inappropriate use of e-mail, the Internet, or the network for users to access, download or transmit any material which might reasonably be considered to be unacceptable i.e., obscene, abusive, sexist, racist or defamatory. You should be aware that such material may also be contained in jokes sent by e-mail. Such misuse of electronic systems will be regarded as a disciplinary matter. Inappropriate material also includes chat, chain mail or global mailings unless for academic purposes.

4.6 Huish reserves the right to use the content of any user's e-mail, storage, and Microsoft Teams conversations in any disciplinary process.

# 5. Use of the Internet

5.1 The College's primary internet access is provided by JISC. They operate the Joint Academic Network (JANET).

5.2 JANET requires connected organisations to agree to abide by and adhere to various terms and conditions when using the service. Details of which can be found at https://community.jisc.ac.uk/library/acceptable-use-policy

5.3 The sites accessed by you, using the Huish internet connection, must comply with the restrictions set out in these guidelines. You must not access or attempt to access unsuitable or inappropriate sites by searching or trying to bypass filters. Accessing inappropriate sites may lead to disciplinary action.

5.4 Huish reserves the right to filter all Internet content electronically to ensure it meets the requirements of this policy. Whilst every effort is made to remove such content, it is not technically possible to ensure that such filtering will stop 100% of such content.

5.5 The use of Virtual Private Network (VPN) software without consent from the IT team is prohibited.

# 6. Use of Email and Microsoft Teams

6.1 E-mails and Microsoft Teams messages should be drafted with care. Due to the informal nature of these forms of communication, it is easy to forget that it is a permanent form of written communication, and that material can be recovered even when it is deleted from your computer.

6.2 Users should not make derogatory remarks in e-mails, on websites, or Microsoft Teams conversations about employees, users or any other person. Any written derogatory remark may constitute libel.

6.3 By sending e-mails and Microsoft Teams messages on the Huish system, you are consenting to the processing of any personal data contained in that e-mail or message and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail or message. If you do not wish Huish to process such data, you should communicate it by other means.

6.4 Any emails sent outside the Huish IT network are accompanied by a Huish standard user notice.

# 7. Copyright and Downloading

7.1 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not printed, forwarded, or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

7.2 Software or Internet applications must never be downloaded without the agreement of the IT team as it may break copyright agreements and could pose a serious risk to network security.

# 8. Legal

8.1 The use of the Huish computer and telephone networks and systems are covered by UK National legislation, including:

- **UK Data Protection Act 2018 and UK GDPR**
  Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 2018.
  Most processing of personal data is subject to the UK General Data Protection Regulations (GDPR). Any person wishing to use facilities for such a purpose are required to inform the Director of IT and Facilities and Director of MIS in advance and comply with any restrictions that the College or the UK Data Protection Commissioner may impose concerning the manner in which data may be held or processed.

- **Copyright Designs & Patents Act 1988**
  Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual, or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a program into the random-access memory or other temporary storage device of a computer or onto any form of permanent data storage medium.

- **Computer Misuse Act 1990**
  - Under the Act hacking and the introduction of viruses are criminal offences. The Act identifies three specific offences:
  - Unauthorised access to computer material (that is, a program or data). e.g., accessing another person's area without permission, trying to steal a password, outputting data to screen or printer
  - Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime e.g., trying to access financial or administrative records with intent.
  - Unauthorised modification of computer material. e.g., modifying records, creation, or introduction of a local or network virus, deliberately generating information to make a system malfunction, using ransomware to encrypt files.

- **Offensive material legislation includes**
  Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984, which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

- **Prevent Duty**
  From 1 July 2015 all schools registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

# 9. Safeguarding and Prevent Duty

9.1 All official Huish communication is via Huish supplied email addresses and Huish systems, this may contain personal or sensitive information that must stay within Huish systems and not copied to personal devices.

9.2 Web browsing reports are regularly reviewed to help keep staff and students safe from terrorist and extremist material.

# 10. E-Safety

10.1 All users must not take, use, share, publish or distribute images or videos of others without their permission.

a. Care should be taken when taking digital or video images that students and staff are appropriately dressed and are not participating in activities that might bring the individuals or Huish into disrepute.

10.2 Personal communications are those made via a personal social media account (including personal messaging accounts, e.g., email, SMS, WhatsApp etc). In all cases, where a personal account is used which associates itself with the college or impacts on the college, it must be made clear that the member of staff or student is not communicating on behalf of the college with an appropriate disclaimer.

10.3 All communications between staff, students and governors should only be made using official Huish systems or approved methods of communication.

10.4 Cyber bullying is any form of bullying which takes place online or through smartphones and tablets. Social networking sites, messaging apps, gaming sites and chat rooms such as Meta, Xbox Live, Instagram, YouTube, Snapchat, and online chat rooms. Where appropriate, cyber bullying will be investigated and could lead to disciplinary action.

10.5 Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from Huish devices and all other technical systems and would lead to criminal prosecution. Other activities e.g., cyber-bullying could lead to criminal prosecution.

10.6 To report any misuse please contact your Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Lead (DDSL). They will decide if any further action is required.

# 11. Cyber Security

11.1 Users should note that all files and emails are scanned electronically for viruses, SPAM, and other unwanted content. If you are suspicious of the contents of a file or email, please contact the IT helpdesk.

11.2 When using your own device to access Huish data or services students should, and staff must, ensure that the device you are using to connect has an in-support operating system, receives regular security updates, system patches, and anti-virus / malware protection. This includes accessing cloud data such as Office 365 documents and email.

11.3 Staff and governors, at Richard Huish College, are not permitted to directly connect to any IT system that hosts Huish organisation data using a personal device that has a Windows or MacOS operating system.

11.4 You are responsible for the security of any data that you take offsite. This could be on a mobile device, external storage device or cloud service platform. If data on external storage is personal or sensitive the data must be encrypted.

11.5 If you are suspicious of the contents of a website, please contact the IT helpdesk.

11.6 To access Huish systems off campus. i.e., from home. You must enable Multifactor Authentication (MFA).

# 12. IT Third Parties

IT third parties are external organizations that provide IT-related products or services to another company. This can include cloud service providers, software vendors, managed service providers, and outsourced development teams.

12.1 Only staff are permitted to request to sign up to any IT third party product or service that will handle or view Huish organisation data.

12.2 To request this permission, the staff member will need to inform the Director of MIS and the Director of IT and Facilities. This will start a process by which all the relevant information can be collected regarding the third-party provider, such as, GDPR, cyber security, compatibility, accessibility, cyber essentials certification, ISO 27001 certification.

12.3 If the third-party provider requires access to Huish systems, for example, for supporting an IT system hosted on Huish hardware, then additional information will be required. Such as external IP addresses, names of IT technicians providing the support.

12.4 Any remote support sessions must first be authorised by IT staff or the system Administrator. Deputy system administrators can be named for when the system administrator is not available and failing that the Director of IT and Facilities or Network Infrastructure Manager can authorise on their behalf in emergency circumstances.

12.5 Remote support sessions must be supervised by Huish staff.

12.6 User accounts required for remote support sessions from third parties must only be enabled for the time they are required for that session.

# 13. Related Policies and Documents

Data Protection and Freedom of Information Policy
Mobile Device Guidance

## APPENDIX 1 – Acceptable Use Agreement (KS1/KS2 pupils and parents/carers)


### ACCEPTABLE USE AGREEMENT FOR (KS1/KS2 PUPILS AND PARENTS / CARERS)

**When I use the school's IT computers / tablets and get onto the internet in school I will:**

- Ask a teacher or suitable adult if I want to use the computers/tablets
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after the school equipment and tell a teacher straight away if something is broken or not working properly
- If issued with a username and password:
  - Only use the username and password I have been given
  - Try my hardest to remember my username and password
  - Never share my password with anyone, including friends
- Never give my personal information (my name, address, or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school systems
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it.

**I agree that the school will monitor the websites I visit and that I may not be allowed to use the IT systems if I don't follow the rules.**

| **Name of pupil:** | |
|---|---|
| **Signed (pupil):** | **Date:** |

**Parent/carer agreement:** I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of staff. I agree to the conditions set out above for pupils using the school's IT systems and internet and will make sure my child understands these.

| **Signed (parent/carer):** | **Date:** |
|---|---|

# APPENDIX 2 – Acceptable Use Agreement (KS3/KS4 pupils)

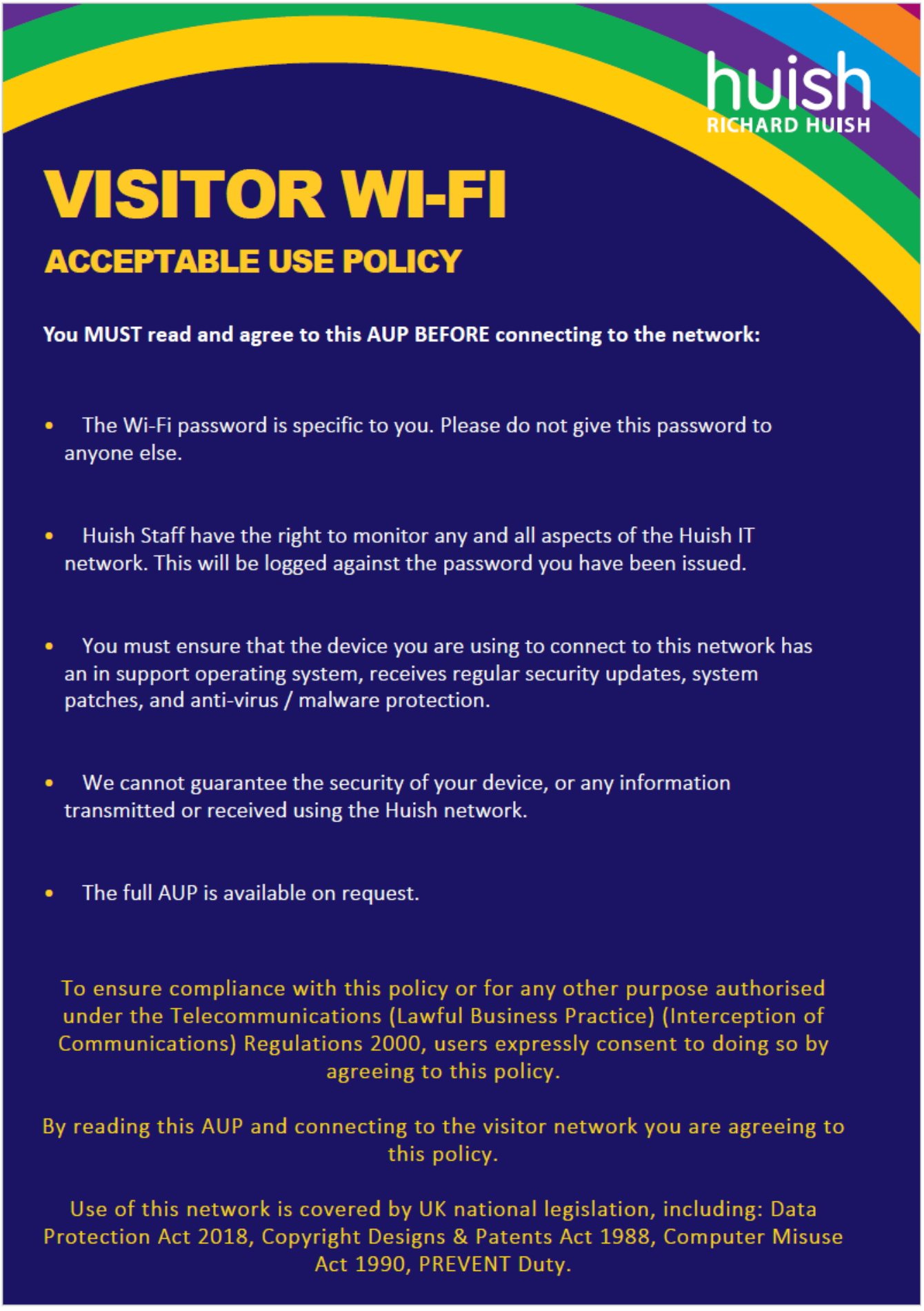
## ACCEPTABLE USE AGREEMENT FOR (KS3/KS4 PUPILS)

- I will only use the school's computers for appropriate school activities and learning.
- I am aware that the school can monitor my computer and network access, including internet and email usage.
- I will not bring files into school via removable media or online storage that can harm the school network or be used to circumvent school security and/or filtering settings.
- I will not try to bypass the school's security or content filters or try to access information which is not allowed.
- I will only edit or delete my own files and not view or change other people's files or user areas without their permission.
- I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my age.
- I will only email or contact people I know, or those approved as part of learning activities.
- When using video chat software, I will ensure that I follow school rules for safe use.
- The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
- I will not give out any personal information that could be used to identify me, my family, or my friends on any online space, unless a trusted adult has given permission to do so.
- If I see anything I am unhappy with or receive a message that makes me feel uncomfortable, I will not respond to it, I will save it and talk to a trusted adult.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I will never arrange to meet someone I have only ever previously met on the Internet including by email or in a chat room, unless I take a trusted adult with me.

**Remember**
**There are laws protecting the use of IT.**
**Computer Misuse Act 1990**
**Copyright Designs & Patents Act 1988**
**UK Data Protection Act 2018 and UK GDPR**

| | |
|---|---|
| **Name of pupil:** | **Tutor Group:** |
| **Signed (pupil):** | **Date:** |

## APPENDIX 3 – Visitor Wi-fi acceptable use policy



## APPENDIX 4 – Summarised AUP

huish
RICHARD HUISH

# SUMMARISED

## ACCEPTABLE USE POLICY

**You MUST read and agree to this AUP BEFORE connecting to the network:**

- You must not access or attempt to access unsuitable or inappropriate sites by searching or trying to bypass filters.
- Huish Staff have the right to monitor any and all aspects of the Huish IT network. This will be logged against the password you have been issued.
- You are not permitted to download/import/install any application/program to a Huish device which has not previously been approved of by the IT Services team.
- There shall be no expectation of privacy when using Huish owned devices and services. Accordingly, users shall not have an expectation of privacy in anything that they create, place on, store, send, or receive on any Huish owned devices and services.
- The full AUP is available on request.

To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, users expressly consent to doing so by agreeing to this policy.

By reading this AUP and connecting to the visitor network you are agreeing to this policy.

Use of this network is covered by UK national legislation, including: Data Protection Act 2018, Copyright Designs & Patents Act 1988, Computer Misuse Act 1990, PREVENT Duty.