Agenda Item 6

Sheffield
City Council

# Audit and Standards Committee Report

**Report of:** **Director of Business Change and Information Solutions**

**Date:** **26/11/2020**

**Subject:** **Information Governance Annual Report**

**Author of Report:** **Mark Gannon**
**Director of Business Change and Information Solutions,**
**Senior Information Risk Owner**

**Summary:**

Information Governance is the generic term used to describe how an organisation manages its information, particularly in respect to legislative and regulatory requirements. This report seeks to provide assurance around the policies, processes and practices employed to ensure we meet those requirements.

**Recommendations:** to note the annual information governance update

**Background Papers:** None

**Category of Report:** OPEN

## Statutory and Council Policy Checklist

| |
|---|
| **Financial Implications** |
| NO: |
| **Legal Implications** |
| YES |
| **Equality of Opportunity Implications** |
| NO |
| **Tackling Health Inequalities Implications** |
| NO |
| **Human rights Implications** |
| NO |
| **Environmental and Sustainability implications** |
| NO |
| **Economic impact** |
| NO |
| **Community safety implications** |
| NO |
| **Human resources implications** |
| NO |
| **Property implications** |
| NO |
| **Area(s) affected** |
| None |
| **Relevant Cabinet Portfolio Member** |
| Terry Fox |
| **Is the item a matter which is reserved for approval by the City Council?** |
| NO |
| **Press release** |
| NO |

**REPORT TITLE: Information Governance Annual Report for 2019/20**

| **1.0** | **INTRODUCTION** |
|---|---|
| | |
| 1.1 | This report has been written to provide an overview of the Information Governance arrangements and performance at the Council for the last financial year and to provide assurance around the policies, processes and practices employed to ensure we meet our legal requirements.<br>It is important to note that this is a retrospective report, covering the year 2019/20. Therefore, this report does not include the impacts of COVID-19 on performance. This report is also being presented later than planned due to the information Management Team needing to prioritise their efforts on COVID-19 response activity since March 2020. In addition, the Team Manager post had been vacant but has now been recruited to.<br>The next retrospective annual report - covering 2020/21 – and future reports will be presented following the normal timescales. The next annual report will include the impact of COVID-19. |
| | |
| **2.0** | **BACKGROUND** |
| | |
| 2.1 | Information Governance is a common term for the distinct, but overlapping disciplines of data protection, access to information, information security, investigatory powers, information and records management, information sharing, information quality and information assurance. |
| | |
| 2.2 | The ultimate purpose of Information Governance is to help an organisation to understand its information needs and responsibilities, to define the rules for the management of information flowing in, out and around the business, and to maximise the value of information while minimising the risks. |
| | |
| 2.3 | Effective Information Governance enables the Council to understand and comply with its legal and administrative obligations, manage and reduce risks, protect privacy and confidentiality, and support services to deliver to the right people at the right time. |
| | |
| 2.4 | The Information Governance landscape is complex and subject to laws, regulations and recommended codes of practice. The key laws include the General Data Protection Regulation 2016/679 (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), and Regulation of Investigatory Powers Act 2000 (RIPA). The Council can be called upon to demonstrate its compliance with these laws and regulations by members of the public, partner agencies, accrediting bodies, and regulators such as the Information Commissioner’s Office, the Surveillance Camera Commissioner and the Investigatory Powers Commissioner. These commissioners have powers to |

| | |
|---|---|
| | impose penalties, including monetary penalties and custodial sentences, on organisations or individuals who breach the laws and regulations. |
| | |
| 2.5 | To enable the Council to understand and shape the Information Governance activity across the Council and ensure compliance, it has nominated specific information governance roles to officers: Senior Information Risk Owner, Portfolio Information Risk Owners, Caldicott Guardians, Senior Responsible Officer (RIPA) and the Data Protection Officer. These roles attend the Information Governance Board, which is subsequently supported by key officers and working groups to help embed information governance practice. In 2019/20, the Council nominated its Directors to become Information Asset Owners and gave them responsibility for managing risks to the personal data and business critical information held within their services. |
| | |
| **3.0** | **DATA PROTECTION LAWS** |
| | |
| 3.1 | 2019/20 was the second financial year in which the General Data Protection Regulation (GDPR) 2016/679 and the Data Protection Act (DPA) 2018 have been in force. The Council has continued to work to ensure compliance with the law and an ongoing GDPR Action Plan is in place. |
| | |
| 3.2 | Data protection compliance remains a key priority for the Council and is currently logged on the Council's Risk Register (Resources Risk ID 352 – High). Work will continue throughout 2020/21 to ensure good practice is understood and embedded into business as usual and that the right evidence is available as and when required to reduce the risk to an acceptable level. |
| | |
| **4.0** | **SUBJECT ACCESS REQUESTS** |
| | |
| 4.1 | Data protection law provides data subjects with a number of rights to better understand and make decisions about the personal data a Data Controller processes about them (Articles 14-22 GDPR). The most commonly used right is Article 15, the right of access, which is known as a Subject Access Request (SAR). |
| | |
| 4.2 | All SARs are logged by the Council's Information Management Team, triaged, and allocated to individual services to provide a response. |
| | |
| 4.3 | SARs must be answered within a legal time limit. The Council's Information Governance Board has set the target that 85% of SARs should be answered in time. Prior to 2019/20, the Council did not manage to reach this target, and the handling of SARs had been logged as a risk on the Corporate Risk Register and reported to EMT because the Council's performance level (Resources Risk ID 196). |
| | |

4.4 In 2019/20, the Council handled 378 Subject Access Requests and answered 85% in time (see Appendix A). This is a significant improvement on previous years; in 2017/18, the Council received 196 requests and 49% were answered in time, and in 2018/19, 294 requests were received with 74% being answered in time.

2019/20 is the first time the Council has met the target of responding on time to more than 85% of requests. This is a particularly noteworthy achievement considering that the Council received 84 more requests in 2019/20 than in 2018/19.

The improved performance statistics are evidence of the effectiveness of measures which were put in place during 2018 in response to the Information Commissioner's Office's (ICO) monitoring of the Council's handling of SARs. These measures included updates to processes and procedures, and commitment of more resources, in particular to help deal with requests for historic social care children's information, which are often complex and time-consuming because the information can span many years and include very sensitive material about the data subject and third parties that needs to be read and redacted before disclosure.

4.5 In addition to the above, the ICO has corresponded with the Council on three separate occasions concerning Subject Access Requests received in 2019/20. The cases concerned situations where individuals complained to the ICO that they were not provided with all of the information to which they were entitled. The ICO upheld one complaint and required the Council to disclose further information to the data subject. In the other two cases, the ICO were satisfied that the Council responded appropriately to the request.

4.6 The handling of SARs remains a priority for the Council.

## 5.0 FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION (EIR) REQUESTS

5.1 The Council is legally required to respond to requests for information under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). Responses must be made within 20 working days, subject to some exceptions. Each response must confirm if the information is held and then either provide the information or explain the reasons why it cannot be disclosed (exemptions/exceptions).

5.2 FOI and EIR requests are logged by the Council's Information Management (IM) Team and then triaged and allocated to individual services to gather the information. Services provide a response to the IM Team, who check this, advise on the application of any exemptions/exceptions and then respond to the customer.

5.3 In 2019/20, the Council received 1941 requests and answered 93.25% in time (appendix B). This response rate is down from 97.1% in 2018/19 and fails to meet the Information Governance Board's target of response rate of 95% of requests answered in time.

5.4 Of the 125 requests which were answered late, at least 83 had the reason for delay listed as being a delay in the relevant service within the Council providing the information to the Information Management Team.

5.5 The FOI and EIR give a requester the right to appeal about the way their request has been handled. This is known as an Internal Review. One of the Council's aims for 2019/20 was to reduce the number of internal reviews and ICO enquiries.

The Council has handled 63 Internal Reviews from requests that were received in 2019/20, 21 fewer than the 84 handled in 2018/19. Of the 63 Internal reviews received, the majority were resolved: either the Council changed its position and released information or upheld the original decision and was accepted by the requester.

5.6 In addition to the above, the ICO has corresponded with the Council on nine separate occasions concerning FOI/EIR requests received in 2019/20. Of these nine cases, the Council resolved two informally with the customer and the ICO upheld two cases in favour of the Council. At the time of this report, five cases remain open and are either awaiting action by an ICO case officer or are awaiting formal closure.

## 6.0 OPEN DATA

6.1 Under the Freedom of Information Act 2000, Protection of Freedoms Act 2012, and the Local Transparency Code 2015, the Council is required to publish certain information on its website or open data sites. The Council is committed to open data to support its transparency agenda and routinely publishes information about its services, key decisions and expenditure.

6.2 The risk relating to the publication of data on the Council's open data sites, including deciding what data should be published and ensuring that published data is accurate, meaningful, owned and regularly updated, remains logged on the Corporate Risk Register (Resources Risk ID 366 - Moderate).

In 2019/20, the Council has continued to work on improving its publication of open data, which has included reviewing the open data sites it uses. Having previously moved its open data from Socrata to ESRI, the Council decided that another site was needed alongside ESRI to make data more accessible to the public.

| | |
|---|---|
| | Consequently, the Council decided to move some of the datasets it makes available via open data, including its FOI Publication Scheme, to a site called Data Mill North. This site allows the publication of 30 datasets and allows more straightforward metadata tagging, so it is felt that it provides a more user-friendly experience. ESRI will continue to be used for the publication of geospatial datasets. |
| | |
| 6.3 | To date approximately 20 datasets have been published onto ESRI site and 10 datasets have been published on Data Mill North. Further work is required to encourage services within the Council to recognise the benefits of open data to help demonstrate the Council's commitments to openness, transparency and public accountability. |
| | |
| **7.0** | **INFORMATION SECURITY INCIDENTS AND PERSONAL DATA BREACHES** |
| | |
| 7.1 | The Council is required to log, assess and mitigate information security incidents and personal data breaches. Incidents can be events that have happened or near misses that affect or are likely to affect the confidentiality, integrity and availability of information. Where an incident occurs and affects personal data, this is a personal data breach. Data protection law requires organisations to notify the Information Commissioner's Office of the personal data breaches that have a high and ongoing risk to the data subjects affected. |
| | |
| 7.2 | In 2019/20, 231 incidents were logged through the Council's information security incident process; 92 of these incidents were classed as personal data breaches (see Appendix C1). The majority of the breaches involved customer personal data and were caused by human error with emails or post being delivered to the wrong person. Of these breaches, five were considered to meet the serious threshold and were reported to the Information Commissioner's Office. None resulted in subsequent action by the regulator (see Appendix C2). |
| | |
| 7.3 | The Information Commissioner has the power to take enforcement action against an organisation for non-compliance with data protection law, which includes data breaches. |
| | |
| 7.4 | Incidents and data breaches have been reported by all Portfolios. The Services that handle sensitive personal data are at greater risk because an incident or breach is more likely to have a greater impact on the customer or data subject and therefore meet the threshold to notify the Information Commissioner. |
| | |
| 7.5 | Consequently, there is a continuing and critical need to manage the information we have, safely and securely, to continue to implement sound data protection practice, and to ensure all staff are aware of their |

| | |
|---|---|
| | responsibilities and have received and completed all the necessary training relevant to their role. |
| | |
| **8.0** | **INVESTIGATORY POWERS COMMISSIONER** |
| | |
| 8.1 | The Council is entitled to use the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 to carry out covert surveillance as part of its statutory duties.  All applications must be approved by a Magistrate before covert surveillance can be carried out. |
| | |
| 8.2 | The Council must fully document all the applications it makes for covert surveillance including the use of Covert Human Intelligence Sources and make the documents available for inspection when required.  The Council makes an annual return to the Investigatory Powers Commissioner's Office, which confirms the number of applications that have been considered and submitted to a Magistrate (see appendix D). |
| | |
| 8.3 | In 2019/2020, the Council made three applications for Directed Surveillance that were all granted by the Magistrate and have since been cancelled; the term cancelled meaning that the period of time in which the Council is authorised to carry out the surveillance has expired. |
| | |
| 8.4 | The Investigatory Powers Commissioner has the power to inspect an organisation to ensure its covert surveillance process and documentation is in place and compliant with the law.  The Council was inspected on 9 January 2017 and inspections usually occur on a three year cycle. |
| | |
| 8.5 | The Council continues to review its covert surveillance governance arrangements and, during 2019/20, conducted two surveillance activities under the Directed Surveillance Authorisations. |
| | |
| **9.0** | **INFORMATION GOVERNANCE RISK AND ISSUES** |
| | |
| 9.1 | In 2019/20, the Council logged a number Information Governance Risks and Issues on its Risk Register.  These varied in severity – High to Low – covering themes including: GDPR, IT Transition and Cyber Security. |
| | |
| 9.2 | The risks are reported to the relevant senior managers every quarter – Senior Management Teams or the Executive Management Team – to ensure the risks are being progressed or to highlight any issues that affect the treatment plan.  The Information Governance Risks are also reported to the Information Governance Board with an accompanying report to confirm the status of the risk and issue including the impact of the treatment and residual risk. |
| | |
| **10.0** | **INFORMATION SECURITY & CYBER SECURITY** |

| | |
|---|---|
| | |
| 10.1 | Information security is about the protection of information or, more specifically, its confidentiality, integrity or availability.  The Council is required to take appropriate security measures to protect information, particularly personal data, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information transmitted, stored or otherwise processed. |
| | |
| 10.2 | During the period the Council has migrated the majority of its IT provision from Capita – although at the time of this report a number of IT services were still in the process of migration. The insourcing of IT from Capita has resulted in changes in IT infrastructure and as the Council is responsible for its own IT it has had to review its assets, processes and security provisions. This is ongoing, however a number of developments which will be delivered in the next period such as the deployment of Office 365, which will provide the Council with additional security tools. |
| | |
| 10.3 | A key component of the Council's resilience is to update its Windows estate – during the period Windows 7 fell out of mainstream support from Microsoft. Due to its enterprise agreement with Microsoft the Council has an additional 12-month grace period from Jan 2020 to Jan 2021 when it will still receive critical security update. However, during the period 2019/20 the Council has been planning its migration to Windows 10 with the anticipation that all Windows 7 devices will be removed from the Councils estate prior to the end of the support period. |
| | |
| 10.4 | Cyber Security is a sub-set of Information Security and focuses on the protection of ICT systems and their components (i.e. hardware, software, data and infrastructure).  The Council logged Cyber Security as a corporate risk in 2016 following Government advice that cyber security was a national threat (Resources Risk ID 290 – High). |
| | |
| **10.5** | The issue of cyber security is an ever-present risk. The likelihood of a cyber-attack is considered high by security experts as attacks constantly become more sophisticated. New threats continue to develop including the potential for state sponsored cyber-attacks and the impact of cyber attacks can be very high. However, by volume, the largest cause of security incidents remains human error. During the period the Council has been working to develop its Information Governance training with a view to re-enforcing the education around information governance to attempt to reduce the number of security incidents derived from human error and increase training and monitoring of training compliance is anticipated to be implemented during the next period as this is a key requirement for programmes such as working with the NHS. |
| | |
| **11.0** | **RECORDS MANAGEMENT** |
| | |

| | |
|---|---|
| 11.1 | Records Management is the practice of managing records with the intention of ensuring they are accurate, reliable and available until they are disposed of or permanently preserved. Effective records management can underpin business practice, support decision making, and improve efficiencies, whereas ineffective records management can hinder operations and present a risk. |
| | |
| 11.2 | The Council continues to provide guidance, training and awareness, explore better use of information technology to automate records management processes, especially retention and disposal and gain a better understanding of management responsibility to own the information processed within their service area. |
| | |
| **12.0** | **TRAINING** |
| | |
| 12.1 | Information governance is essential to ensure staff and other authorised users or processers of council information or systems understand and accept their responsibilities to handle information lawfully and safely. In the event of any complaint, incident or data breach, the Information Commissioner's Office ask for confirmation as to what training provision is in place and whether the employee involved in the matter has completed the training available. |
| | |
| 12.2 | The Council has a range of information governance related training, from general awareness courses to bespoke sessions on key topics. General training includes the Information Management e-learning and Regulation of Investigatory Powers e-learning, which are available thought the Sheffield Development Hub. Bespoke training has also been available and delivered to officers needing greater knowledge in key governance areas, including data protection, data protection impact assessments, privacy notices, information sharing, etc. |
| | |
| 12.3 | The take up and completion of information governance training varies. For example, the Information Management e-learning module is mandatory for all employees and authorised users using council information, but figures provided by HR in April 2020 confirmed that 64% of staff had completed the training. While this is an increase of 15% from March 2019, it still falls short of the 100% target. In contrast, attendance to taught courses has proven to be more popular, but each session is only delivered to a small audience. |
| | |
| 12.4 | The matter has been raised at the Information Governance Board and there will be a greater push for staff to be made aware of the training that is available and to increase the completion numbers. This will include reviewing and possibly changing the existing training methods to enable services to develop the relevant knowledge and skills to embed information governance in their working life and better protect the information they handle and ultimately our customers. |

**Appendix A: FOI and EIR Requests Response Performance 2019/20**

| | | Responses Issued* | | | | |
|---|---|---|---|---|---|---|
| | Requests Received | Within 20 days | Overdue | Total | % of Responses Issued which were issued within 20 days | % of Responses Issued which were overdue |
| Qtr 1 | 493 | 464 | 15 | 479 | **96.87%** | **3.13%** |
| Qtr 2 | 497 | 468 | 23 | 491 | **95.32%** | **4.68%** |
| Qtr 3 | 458 | 409 | 39 | 448 | **91.29%** | **8.71%** |
| Qtr 4 | 493 | 385 | 48 | 433 | **88.91%** | **11.09%** |
| **Total** | **1941** | **1726** | **125** | **1851** | **93.25%** | **6.75%** |

**Appendix B-1: Subject Access Request Performance 2019/20**

| 2019/20 | Received | Answered in time | Answered Late | In Progress in time | In Progress, but late | Compliance % |
|---|---|---|---|---|---|---|
| **Qtr 1** | 94 | 88 | 6 | 0 | 0 | **94%** |
| **Qtr 2** | 82 | 66 | 16 | 0 | 0 | **80%** |
| **Qtr 3** | 74 | 70 | 4 | 0 | 0 | **95%** |
| **Qtr 4** | 99 | 73 | 10 | 0 | 16 | **74%** |
| **Total** | **349** | **297** | **36** | **0** | **16** | **85%** |

## Appendix C: Reported Information Security Incidents and Personal Data Breaches

### C-1 Quarterly Figures

| Type of Incident by Quarter | No. of Incidents | No. of Data Breaches | No. of ICO Notifications |
|---|---|---|---|
| **Q1** | **38** | **20** | **2** |
| Cyber Attack (e.g. virus, ransomware, phishing email) | 1 | 0 | 0 |
| Information disclosed in error | 30 | 18 | 2 |
| Lost in transit or away from the office | 1 | 0 | 0 |
| Lost or stolen paperwork | 3 | 1 | 0 |
| Non-secure disposal of paperwork | 1 | 1 | 0 |
| Unauthorised access to IT systems | 2 | 0 | 0 |
| **Q2** | **58** | **33** | **1** |
| Cyber Attack (e.g. virus, ransomware, phishing email) | 1 | 0 | 0 |
| Information disclosed in error | 45 | 28 | 0 |
| Lost in transit or away from the office | 1 | 0 | 0 |
| Lost or stolen paperwork | 4 | 3 | 1 |
| Online Disclosure (e.g. website, social media) | 1 | 0 | 0 |
| Unauthorised access to IT systems | 6 | 2 | 0 |
| **Q3** | **57** | **20** | **1** |
| Corruption or inability to recover information | 2 | 0 | 0 |
| Information disclosed in error | 41 | 17 | 0 |
| Lost in transit or away from the office | 1 | 0 | 0 |
| Lost or stolen hardware | 2 | 0 | 0 |
| Lost or stolen paperwork | 6 | 2 | 1 |
| Non-secure disposal of paperwork | 2 | 0 | 0 |
| Unauthorised access to IT systems | 2 | 1 | 0 |
| Unauthorised access to physical documents | 1 | 0 | 0 |
| **Q4** | **78** | **19** | **1** |
| Cyber Attack (e.g. virus, ransomware, phishing email) | 1 | 0 | 0 |
| Information disclosed in error | 64 | 15 | 0 |
| Lost or stolen hardware | 1 | 0 | 0 |
| Lost or stolen paperwork | 5 | 2 | 1 |
| Non-secure disposal of hardware | 1 | 0 | 0 |
| Non-secure disposal of paperwork | 1 | 0 | 0 |
| Online Disclosure (e.g. website, social media) | 2 | 2 | 0 |
| Unauthorised access to IT systems | 2 | 0 | 0 |
| Unauthorised access to physical documents | 1 | 0 | 0 |
| **Grand Total** | **231** | **92** | **5** |

## C2 – Summary of personal data breaches investigated by the ICO

| SCC Ref. | Case Opened | Summary of the personal data breaches investigated by the Information Commissioner's Office | INCIDENT TYPE |
|---|---|---|---|
| 2019/17 | 26/04/2019 | 279 parking PCN letters were printed double-sided instead of single-sided. This resulted in around 140 people receiving the names, addresses, and registration numbers of other people. One individual contacted the ICO. The ICO took no further action. | Disclosed in Error |
| 2019/23 | 09/05/2019 | Tribunal documents were sent to four individuals (or their appointees) involved in a Housing Benefit appeal. The documents included information about each of the individuals, so all four people had access to each other's health and financial information. The Council reported the breach to the ICO and contacted the affected parties to ask for the documents to be returned. The ICO took no further action. | Disclosed in Error |
| 2019/92 | 11/09/2019 | A social worker's car was broken into and information about individual service users was stolen. The Council reported the breach to the ICO and notified the affected parties. The Council reviewed its practice and issued internal guidance about remote working with paper documents. The ICO took no further action. | Lost or Stolen Paperwork |
| 2019/145 | 25/11/2019 | Education, Health & Care (EHC) Plans were posted to a family, but the posted documents never arrived. The Council reviewed its practice and issued internal guidance about sending sensitive documents via tracked post. The ICO took no further action. | Lost or Stolen Paperwork |
| 2019/209 | 18/02/2020 | A social worker's house was broken into and the officer's paper notebook and phone were stolen. The Council reported the breach to the ICO. The ICO took no further action. | Lost or Stolen Paperwork |

## Appendix D: Investigatory Powers Commissioner Office Return

| Sheffield City Council | | Volume |
|---|---|---|
| Covert Human Intelligence Sources (CHIS) & Juvenile Covert Human Intelligence Sources (Juvenile CHIS) | The number of applications made for a CHIS authorisation? | 0 |
| | Of these, the number of applications made for a Juvenile CHIS authorisation? | 0 |
| | The number of CHIS authorisations successfully granted? | 0 |
| | Of these, the number of Juvenile CHIS authorisations successfully granted? | 0 |
| | The number of urgent applications made for a CHIS warrant? | 0 |
| | Of these, the number of urgent applications made for a Juvenile CHIS authorisations? | 0 |
| | The number of CHIS authorisations granted in an urgent case? | 0 |
| | Of these, the number of Juvenile CHIS authorisations granted in an urgent case? | 0 |
| | The number of CHIS authorisations that were renewed? | 0 |
| | The number of CHIS authorisations that were cancelled? | 0 |
| | The number of CHIS authorisations extant at the end of the year? | 0 |
| | The age of the Juvenile CHIS at the time of the authorisation's issue? (to be completed in rows below) | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| | Juvenile CHIS age at application | 0 |
| | Quantity | 0 |
| Directed Surveillance (RIPA & RIPSA) | The number of applications made for a Directed Surveillance authorisation? | 3 |
| | The number of Directed Surveillance authorisations successfully granted? | 3 |
| | The number of urgent applications made for a Directed Surveillance authorisation? | 0 |
| | The number of Directed Surveillance authorisation granted in an urgent case? | 0 |
| | The number of Directed Surveillance authorisations that were cancelled? | 3 |
| | The number of Directed Surveillance authorisations extant at the end of the year? | 0 |