POLICY/PROCEDURE INFORMATION (Policy no OP007)	
Subject	**Information Security Policy** *(This policy is non-contractual and is subject to periodic review and will be amended according to service development needs).*
Applicable to	All staff and volunteers of Nottinghamshire Hospice
Target Audience	Others such as agents, consultants and other representatives of Nottinghamshire Hospice may be required to comply with the policy as a condition of appointment.
Date issued	Oct 2021
Next review date	Oct 2022
Lead responsible for Policy	Chief Executive Officer
Policy reviewed by	Risk Evolves October 2021
Notified to (when)	Rachel Hucknall, CEO, October 2021
Authorised by (when)	Strategy Corporate Governance Committee – October 2021
CQC Standard if applicable	
Links to other Hospice Policies	Data protection policy HR0005 Data retention policy OP006 Risk assessment policy OP004 Use of equipment policy HR009
Links to external policies	
Summary	Always check with your Line Manager before taking equipment belonging to Nottinghamshire Hospice out of the building. All equipment should be booked out, signed for and appropriately labelled as the property of Nottinghamshire Hospice.
This policy replaces	

VERSION CONTROL		
Status	**Date**	**Reviewed date**
Original policy written by Kate Rogers, Governance and Operations Manager	Oct 2021	
Policy reviewed by Rachel Hucknall, Chief Executive	Oct 2021	
Policy ratified by Strategy Corporate Governance Committee and added to website	Oct 2021	Oct 2022

Contents

Appendices

1. Introduction

This information security policy is a key component of Nottinghamshire Hospice management framework. It sets the requirements and responsibilities for maintaining the security of information within Nottinghamshire Hospice. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

It is expected that Nottinghamshire Hospices business partners who access the organisations information retains a high-level of information security, and follow all expectations outlined within this policy.

2. Aim and Scope of this policy

- The aims of this policy are to set out the rules governing the secure management of our information assets by:
    - preserving the **confidentiality, integrity and availability** of our business information
    - ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies
    - ensuring an approach to security in which all members of staff fully understand their own **responsibilities**
    - creating and maintaining within the organisation a level of **awareness** of the need for information
    - detailing how to **protect** the information assets under our control
- This policy applies to all information/data, information systems, networks, applications, locations and staff of Nottinghamshire Hospice or supplied under contract to it.

3. Responsibilities

- Ultimate responsibility for information security rests with the Chief Executive of Nottinghamshire Hospice, but on a day-to-day basis the Director of Resources shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by the Director of Resources. Both the Policy and the Risk Register shall be reviewed by Director of Resources at least annually.
- Line Managers are responsible for ensuring that their permanent staff, temporary staff and contractors are aware of:-
    - The information security policies applicable in their work areas
    - Their personal responsibilities for information security
    - How to access advice on information security matters
- All staff shall comply with the information security policy and must understand their responsibilities to protect the company's data. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of information within their business area. Access to departmental information is controlled by

access being approved on an individual basis by the line manager and/or the Director of Resources.

- Each member of staff shall be responsible for the operational security of the information systems they use. There is a security banner in place for all users at log on which confirms there accountability and actions for miss use.
- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Legislation

- Nottinghamshire Hospice is required to abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.
- The requirement to comply with legislation shall be devolved to employees, volunteers and agents of the Nottinghamshire Hospice, who may be held personally accountable for any breaches of information security for which they are responsible.
- In particular, Nottinghamshire Hospice is required to comply with:
  - The Data Protection Act (1998)
  - The Data Protection (Processing of Sensitive Personal Data) Order 2000.
  - The Copyright, Designs and Patents Act (1988)
  - The Computer Misuse Act (1990)
  - The Health and Safety at Work Act (1974)
  - Human Rights Act (1998)
  - Regulation of Investigatory Powers Act (2000)
  - Freedom of Information Act (2000)
  - NHS Data Protection Toolkit – annual compliance review

5. Personnel Security

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the company, their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff. This is in the form of the GDPR training available on Blue Stream Academy.
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary. This includes regular discussions about information security at Corporate Management Team meetings.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved as suitable by the IT contractor and the Director of Finance and Resources. Individual and Nottinghamshire Hospice intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

6. Access Management

Physical Access

- Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data
- All passwords shall be eight characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers
- All administrator-level passwords shall be changed at least every 60 days
    - Where available, two-factor authentication shall be used to provide additional security. This is in place on the 365 portal for IT supplier administration access.
    - All users shall use uniquely named user accounts

- Generic user accounts that are used by more than one person or service shall not be used, with the exception of the below accounts.
    - Maintenance assistant log on using maintenance@nottshopsice.org
    - Training laptops which have no access to the network, use hospicenow\training to log on

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a business need to access the information. Access to departmental information is controlled by access being approved on an individual basis by the line manager and/or the Director of Resources.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Chief Executive.
- A list of individuals with administrator-level access shall be held by the IT contractor and Senior Management and shall be reviewed every 6 months
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges. This access can be requested by contacting the IT contractor and seeking approval from the Chief Executive.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Access is listed on the Information Asset Register.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control

process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- Regular audits of software will be completed by the IT provider (at least monthly)
- Where software has been found to be incorrectly downloaded which does not meet Appex A – Approved Applications List, this will be removed immediately by the IT provider.
- The business reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7. Asset Management

Asset Ownership

- Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

- An accurate record of business information assets, including source, ownership, modification and disposal shall be maintained via the Nottinghamshire Hospice Device and Application List.
- All disposal certificates will be saved in this location; N:\Building and Transport\IT\IT equipment disposal certificates
- All data shall be securely wiped from all hardware before disposal. For computer drives and external disks, this should only be completed by the IT provider.

Asset Handling

- Nottinghamshire Hospice shall identify particularly valuable or sensitive information assets through the use of data classification.
- All sensitive data will be secured with password protection before sending internally and externally.
- Where this data is shared externally with third party suppliers, the privacy statement will be reviewed, and a data sharing contract put in place by the Director of Resource.
- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.
- All company information shall be categorised into one of the three categories in the table below based on the description and examples provided:

Category	Description	Example
Public	Information which is not confidential and can be made available publicly through any channels.	• Details of products and services on the website • Published company information • Social media updates • Press releases
Amber Information	Information which, if lost or or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners	• Company operating procedures and policy • Client contact details • Company plans and financial information • Basic employee information including personal data
Red Information	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	• Client intellectual property • Data in e-commerce systems • Employee salary details • Any information defined as "sensitive personal data" under the Data Protection Act

Removable media

- Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded (e.g. serial number, date, issued to, returned).
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, must be used on the basic Training profile, not attached to the network via Wi-Fi or ethernet cable. This can be achieved by signing in as Training on any of the designated Training laptops. This media will then be scanned using Anti-Virus software.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.
- Users breaching these requirements may be subject to disciplinary action.

Mobile working

- Where necessary, staff may use company-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements

- Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Director of Resources.
- Such devices must have anti-malware software installed (if available for the device), must have a PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the Director of Resources immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal mobile phones to access business email. This usage must be authorised by the Director of Resources. The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy, including having the correct malware and anti-virus installed.
- No other personal devices are to be used to access business information

Social Media

- Social media may only be used for business purposes by using official business social media accounts with authorisation from the Director of Resources. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
- Business social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Director of Resources and/or the Chief Executive.
- Users breaching this requirement may be subject to disciplinary action.

8. Physical and Environmental Management

- In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
- Systems shall be protected from power loss by UPS if indicated by the risk assessment.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

9. Computer and Network Management

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Director of Resources and the Chief Executive.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the Director of Resources with the IT provider.

Accreditation

- The organisation shall ensure that all new and modified information systems, applications and networks include security provisions.
- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Director of Resources before they commence operation.

Software Management

- All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
- All software security updates/patches shall be installed within 7 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes. See Appendix A for an approved list of Software.
- Users shall not install software or other active code on the devices containing business information without permission from the Director of Resources and gaining administration access by the IT provider.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes by the IT provider.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
- A backup copy shall be held in a different physical location to the business premises. This is an offsite at the IT provider.
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g. a ‘cloud provider’) there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- All anti-malware software shall be set to:
    - scan files and data on the device on a daily basis
    - scan files on-access
    - automatically check for, and install, virus definitions and updates to the software itself on a daily basis
    - block access to malicious websites

Vulnerability scanning

- The business shall have a yearly vulnerability scan of all external IP addresses carried out by a suitable external company
- The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities
- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

Penetration Test

- The business may choose to complete a penetration test and scan of all external IP addresses carried out by a suitable external company.

10. Response

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Chief Executive.
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Chief Executive.
- Information security incidents shall be recorded in the Security Incident Log as part of the Incident reporting system, an incident form completed with identifying number and investigated by the Director of Resources and/or the Chief Executive to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.
- The incident response process will be tested annually as a minimum.

Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting

- The Information Security Officer shall keep the business informed of the information security status of the organisation by means of regular reports to senior management.

Further Information

- Further information and guidance on this policy can be obtained from Maria Holmes, Director of Finance and Resources, 0115 910 1008 ext 236. Comments and suggestions to improve security are always welcome.

Appendix A

Nottinghamshire Hospice Approved Applications List

As of October 2021

To be reviewed annually as a minimum

Application Name	Publisher
Adobe Acrobat DC	Adobe Systems Incorporated
Adobe Acrobat DC (64-bit)	Adobe
Adobe Acrobat Reader DC	Adobe Systems Incorporated
Adobe Creative Cloud	Adobe Inc.
Adobe Genuine Service	Adobe
Cisco WebEx Meetings	Cisco WebEx LLC
CSY Vector 7.57 built 03/05/18	CSY Retail Systems Ltd
CutePDF Writer	Acro Software Inc.
DataFlex 2017 Windows Client 19.0	Data Access Worldwide
Dell SupportAssist	Dell Inc.
Dell SupportAssist OS Recovery Plugin for Dell Update	Dell Inc.
donorflex	Care Data Systems
donorflex_Outlook_plugin	Care Data Systems
DrayTek Smart VPN Client	DrayTek Corporation
ESET Endpoint Antivirus	ESET, spol. s r.o.
ESET File Security	ESET, spol. s r.o.
ESET Management Agent	ESET, spol. s r.o.
Gemalto Bluetooth Device Manager	Gemalto
GemPcCCID	Gemalto
Google Chrome	Google LLC
GoTo Opener	LogMeIn, Inc.
GoToMeeting	LogMeIn, Inc.
HP ESU for Microsoft Windows 10	HP
HP LaserJet 400 M401	Hewlett-Packard
HP MAC Address Manager	HP Inc.
HP Officejet Pro 8100 Basic Device Software	Hewlett-Packard Co.
HP Officejet Pro 8100 Help	Hewlett Packard
HP Officejet Pro 8100 Product Improvement Study	Hewlett-Packard Co.
HP Officejet Pro 8600 Basic Device Software	Hewlett-Packard Co.
HP Officejet Pro 8620 Basic Device Software	Hewlett-Packard Co.
HP System Default Settings	HP Inc.
HP Update	Hewlett-Packard
IIS 8.0 Express	Microsoft Corporation
IIS Express Application Compatibility Database for x64	
IIS Express Application Compatibility Database for x86	
Intel(R) Dynamic Platform and Thermal Framework	Intel Corporation
Intel(R) Management Engine Components	Intel Corporation
Intel(R) Network Connections	Intel
Intel(R) Processor Graphics	Intel Corporation
Intel(R) Serial IO	Intel Corporation
Intel(R) Wireless Bluetooth(R)	Intel Corporation
Intel® Driver & Support Assistant	Intel

Intel® Optane™ Pinning Explorer Extensions	Intel Corporation
KONICA MINOLTA C759_C658_C368_C287_C3851Series	KONICA MINOLTA
Lansweeper	Lansweeper.com
Lenovo Vantage Service	Lenovo Group Ltd.
Microsoft 365 - en-us	Microsoft Corporation
Microsoft 365 Apps for business - en-us	Microsoft Corporation
Microsoft 365 Apps for enterprise - en-us	Microsoft Corporation
Microsoft Edge	Microsoft Corporation
Microsoft Edge Update	
Microsoft Edge WebView2 Runtime	Microsoft Corporation
Microsoft ODBC Driver 11 for SQL Server	Microsoft Corporation
Microsoft Office Professional Plus 2010	Microsoft Corporation
Microsoft OLE DB Driver for SQL Server	Microsoft Corporation
Microsoft OneDrive	Microsoft Corporation
Microsoft Report Viewer 2014 Runtime	Microsoft Corporation
Microsoft Report Viewer Redistributable 2005	Microsoft Corporation
Microsoft Search in Bing	Microsoft Corporation
Microsoft Silverlight	Microsoft Corporation
Microsoft SQL Server 2005	Microsoft Corporation
Microsoft SQL Server 2008 R2 Management Objects	Microsoft Corporation
Microsoft SQL Server 2008 Setup Support Files	Microsoft Corporation
Microsoft SQL Server 2012 (64-bit)	Microsoft Corporation
Microsoft SQL Server 2012 Native Client	Microsoft Corporation
Microsoft SQL Server 2012 Setup (English)	Microsoft Corporation
Microsoft SQL Server 2012 Transact-SQL ScriptDom	Microsoft Corporation
Microsoft SQL Server 2014 (64-bit)	Microsoft Corporation
Microsoft SQL Server 2014 Express LocalDB	Microsoft Corporation
Microsoft SQL Server 2014 Management Objects (x64)	Microsoft Corporation
Microsoft SQL Server 2014 Policies	Microsoft Corporation
Microsoft SQL Server 2014 Setup (English)	Microsoft Corporation
Microsoft SQL Server 2014 Transact-SQL Compiler Service	Microsoft Corporation
Microsoft SQL Server 2014 Transact-SQL ScriptDom	Microsoft Corporation
Microsoft SQL Server 2017 (64-bit)	Microsoft Corporation
Microsoft SQL Server 2017 Setup (English)	Microsoft Corporation
Microsoft SQL Server 2017 T-SQL Language Service	Microsoft Corporation
Microsoft SQL Server Management Studio - 18.6	Microsoft Corporation
Microsoft SQL Server Native Client	Microsoft Corporation
Microsoft SQL Server Setup Support Files (English)	Microsoft Corporation
Microsoft SQL Server System CLR Types	Microsoft Corporation
Microsoft SQL Server VSS Writer	Microsoft Corporation
Microsoft Sync Framework 2.0 Core Components (x64) ENU	Microsoft Corporation
Microsoft Sync Framework 2.0 Provider Services (x64) ENU	Microsoft Corporation
Microsoft System CLR Types for SQL Server 2014	Microsoft Corporation
Microsoft Teams	Microsoft Corporation
Microsoft Update Health Tools	Microsoft Corporation
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation
Microsoft Visual C++ 2005 Redistributable (x64)	Microsoft Corporation
Microsoft Visual C++ 2005 Redistributable (x64) - KB2467175	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x64	Microsoft Corporation

Microsoft Visual C++ 2008 Redistributable - x86	Microsoft Corporation
Microsoft Visual C++ 2010 x64 Redistributable	Microsoft Corporation
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Corporation
Microsoft Visual C++ 2010 x86 Runtime	Microsoft Corporation
Microsoft Visual C++ 2012 Redistributable (x64)	Microsoft Corporation
Microsoft Visual C++ 2012 Redistributable (x86)	Microsoft Corporation
Microsoft Visual C++ 2013 Redistributable (x64)	Microsoft Corporation
Microsoft Visual C++ 2015 Redistributable (x64)	Microsoft Corporation
Microsoft Visual C++ 2015 Redistributable (x86)	Microsoft Corporation
Microsoft Visual C++ 2015-2019 Redistributable (x64)	Microsoft Corporation
Microsoft Visual C++ 2015-2019 Redistributable (x86)	Microsoft Corporation
Microsoft Visual C++ 2017 Redistributable (x64)	Microsoft Corporation
Microsoft Visual Studio 2010 Shell (Isolated) - ENU	Microsoft Corporation
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	Microsoft Corporation
Microsoft Visual Studio Tools for Applications 2017	Microsoft Corporation
Microsoft VSS Writer for SQL Server 2014	Microsoft Corporation
Microsoft VSS Writer for SQL Server 2017	Microsoft Corporation
Mozilla Firefox (x64 en-GB)	Mozilla
Mozilla Firefox 60.9.0 ESR (x86 en-US)	Mozilla
Mozilla Firefox 67.0.1 (x64 en-GB)	Mozilla
Mozilla Firefox 68.0.1 (x64 en-GB)	Mozilla
Mozilla Firefox 70.0.1 (x64 en-GB)	Mozilla
Mozilla Firefox 73.0.1 (x64 en-GB)	Mozilla
Mozilla Firefox 79.0 (x64 en-GB)	Mozilla
Mozilla Firefox 81.0.1 (x64 en-GB)	Mozilla
Mozilla Firefox 83.0 (x64 en-GB)	Mozilla
Mozilla Firefox ESR (x64 en-US)	Mozilla
Mozilla Firefox ESR (x86 en-US)	Mozilla
Mozilla Maintenance Service	Mozilla
MyEpson Portal	SEIKO EPSON Corporation
Npcap OEM	Nmap Project
NVIDIA Graphics Driver	NVIDIA Corporation
NVIDIA Update	NVIDIA Corporation
OneStop Collection Agent	Business I.T. Systems Ltd
Outlook2010donorflexAddIn1	Microsoft
Practis	INTEC For Business Limited
PrintProjects	RocketLife Inc.
PuTTY release	Simon Tatham
Qualcomm 11ac Wireless LAN&Bluetooth Installer	Qualcomm
Realtek Audio Driver	Realtek Semiconductor Corp.
Realtek Card Reader	Realtek Semiconductor Corp.
Realtek Ethernet Controller Driver	Realtek
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.
Realtek USB Audio	Realtek Semiconductor Corp.
Sage (UK) Ltd. Sage 50 Payroll	Sage (UK) Ltd.
Sage 50 Accounts	Sage (UK) Ltd.
Sage 50 Accounts Service	Sage (UK) Ltd
Sage 50 HR	Sage (UK) Limited
Sage 50 Payroll	Sage (UK) Ltd.

Sage 50cloud Payroll	Sage (UK) Ltd.
SageSDataServerInstall	Sage
SCFileSecureAES	Secure Collections Ltd
Teams Machine-Wide Installer	Microsoft Corporation
TeamViewer Host	TeamViewer
TeamViewer Monitoring & Asset Management (ITbrain)	TeamViewer
TeamViewer Patch & Asset Management	TeamViewer
ViceVersa Pro 3.0 64-bit (Build 3003)	TGRMN Software
Visual DataFlex 2012 Client Engine 17.1	Data Access Worldwide
VMware Tools	VMware, Inc.
Web Signer Bundle 64 bits Barclays with Classic Client middleware & eSigner	Gemalto
Windows 10 Update Assistant	Microsoft Corporation
Windows Internet Explorer 11	Microsoft Corporation
Windows Setup Remediations (x64) (KB4023057)	
Zoom	Zoom Video Communications, Inc.