New College Durham

Policy on

Information Security

New College Durham is committed to safeguarding & promoting the welfare of children and young people, as well as vulnerable adults, and expects all staff and volunteers to share this commitment.

New College Durham

Information Security

Policy

(Equality and Diversity Assessment)

We will consider any request for this procedure to be made available in an alternative format.

We review our policies and procedures regularly to update them and to ensure that they are accessible and fair to all. All policies and procedures are subject to equality impact assessments. Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a different impact on grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or human rights.

We are always keen to hear from anyone who wants to contribute to these impact assessments and we welcome suggestions for improving the accessibility or fairness of the policy.

To make suggestions or to seek further information please contact:

ICT Department
records@newdur.ac.uk

If any employee has difficulty understanding this policy, please contact the College's ICT Department.

Equality Impact Assessed: August 2017
Accessibility Checked: June 2019

Policy Title	**Information Security Policy**
Document Owner	**Head of ICT**
Owning Directorate	**Corporate Services**
Owning Department	**ICT**

Directorates and Departments affected by this Procedure	**All staff and students**
Procedure Effective From	**September 2015**
Next Review Date	**September 2020**

Contents

1. Introduction 4
2. Scope of the Policy 4
3. Responsibilities 4
4. Relationship with existing and future policies and standards 4
5. Requirements for Information Security 5

A. INFORMATION ACCESS POLICY 7
B. BUSINESS CONTINUITY POLICY 10
C. SOFTWARE MANAGEMENT POLICY 11
D OPERATIONS POLICY 13
E. SYSTEM MANAGEMENT POLICY 15
F. SYSTEM PLANNING POLICY 17
G. REMOTE ACCESS POLICY 19
H NETWORK MANAGEMENT POLICY 20

New College Durham

Information Security Policy

1. Introduction

This Information Security Policy is relevant to all Schools and Departments and to all of the staff within them.

2. Scope of the Policy

It is the policy of the College to ensure that the information it manages is appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of information.

This Policy provides management direction and support for information security across all Schools and Departments.

Information managed by the College is not just held in electronic format and therefore this Policy covers the security of information held on all media.

3. Responsibilities

Responsibility for ensuring compliance with this Policy lies with the Senior Executive Group.

The Senior Information Risk Owner (SIRO) for the College is the Deputy Principal (Human Resources & Corporate Services). The SIRO is responsible for ensuring information security risk assessments are completed, policy breaches are addressed and acts as advocate for information risk management at the highest level.

The ICT department is responsible for the maintenance of this Policy as well as maintaining associated guidelines and promoting compliance with them.

Compliance with this Policy and any associated procedures is compulsory for all staff employed by the College. A member of staff who fails to comply with the Policy may be subjected to disciplinary action under the College disciplinary policy. It is the responsibility of Heads of Departments/School and their Directors to ensure that their staff are made aware of the existence of this Policy and its content.

4. Relationship with existing and future policies and standards

This Policy consists of:

a. Information Access Policy
b. Business Continuity Policy

c. Software Management Policy
d. Operations Policy
e. System Management Policy
f. System Planning Policy
g. Remote Access Policy
h. Network Management Policy

The following College policies and plans are related to this Information Security Policy:

Management and Monitoring of Electronic Communications, Internet and Telephones Policy
Records Management Policy
Data Protection Policy
ICT Business Continuity Plan
ICT Business Impact Assessment

The College will seek to facilitate compliance with BS ISO IEC 27001:2017, BS7799 2:2005 and BS10008:2008. Compliance with this Policy will facilitate compliance with other information-related legislation, especially data protection law.

5. Requirements for Information Security

The Senior Executive Group will ensure there is clear direction, adequate resourcing and visible management support for security initiatives.

The ICT department will devise and co-ordinate the implementation of information security controls according to this Policy. The department will also advise heads of department on any risks arising from the implementation of new systems.

The responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out will lie with the System Owner and the Data Owner[1].

New information systems will be identified and authorised via the Information Management Steering Group. To determine the appropriate levels of security measures applied to information systems, a process of risk assessment will be carried out for each system to identify the probability and impact of security failures. Where Personal Data is held in a system a Data Protection Impact Assessment must also be carried out. Usually the System Owner or Data Owner will carry out these assessments in consultation with the relevant members of the ICT Department.

The risk posed to the College by potential failures in the security of information held in paper or manual systems will also be considered under this Policy.

[1] As denoted in the Information Asset Register

Responsibility for these assessments will lie with the head of the department managing the information.

The College will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies and network and telecommunications operators in respect of this Policy.

7. Obligations for third parties

Where a third party is asked to process data on behalf of the College, the ICT Operations Manager must review the third party's information security arrangements and provide written authorisation for the processing to commence. There is a checklist included at appendix A which should be completed if the third party cannot produce adequate documentation.

8. Evaluation and Review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the Corporation.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

A. INFORMATION ACCESS POLICY

A1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the accessing of information, giving guidance in accordance with current legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. the integrity and security of all electronic systems is maintained;
b. all information is stored in a secure manner and that appropriate safeguards are in place to prevent improper access;
c. any attempts to gain improper access to information are detected and recorded accordingly;
d. College information systems are not compromised or used for unauthorised activities;
e. only authorised members of staff can collect and view pertinent information, which must then only be used for legitimate purposes;
f. information is only relayed to other legitimate and authorised users both inside and outside the College.

A2. Guidance

User Login and Passwords

All users who need access to a computer system within the College are required to have a legitimate user login and password. The College expects all users to adhere to the following guidelines:

a. users will not attempt to gain unauthorised access to College IT systems;
b. passwords must be a minimum of eight characters in length and should be changed every 180 days when prompted;
c. any temporary passwords issued must be changed at first use;
d. passwords must never be written down or disclosed to another individual or organisation;
e. passwords should never be sent in the form of clear text e-mail messages.

Users are responsible for the secrecy and integrity of their passwords. The College will consider password sharing a breach of this Policy and this may result in disciplinary action being taken by the College.

Inactive network accounts will shut down after a defined period of inactivity to prevent unauthorised access.

Security awareness activities will be scheduled on a regular basis and information security training is scheduled as a mandatory activity for all new staff.

External Access to Information

External access to College IT systems is strictly forbidden unless the user has a valid login and password. Any authorised user logging in to the College network from home or from another external access point should only do so in accordance with the guidelines specified in the Remote Access Policy.

Information Access by Third Party Organisations

Access to College IT facilities by third parties will not be provided until a copy of the Acceptable Use Policy has been signed by an appropriate third party representative. The College will also utilise data sharing agreements in all situations when the information being disclosed can be classified as personal or confidential data.

All authorised third parties who require access to IT infrastructure will also be directed to read this Policy and the Data Protection Policy.

(For the process, see appendix B)

Information Access - Incident Reporting

Any IT security incident involving the unauthorised accessing of information within the College must be reported to the Head of ICT as soon as possible. In the event that the Head of ICT is implicated in proceedings, notification of the incident should be made to the SIRO. In the event that both the SIRO and the Head of ICT are implicated, the incident should be reported to the Principal.

The College will aim to assess any reported incidents and will look to ensure that appropriate technical and procedural measures are taken to address identified security weaknesses.

Police Requests

The police will sometimes request information from the College to help with their enquiries. All police requests that are accepted by the College should be handled initially by the Principal's Office and thereafter may be referred to ICT for the provision of data.

Access Levels

Procedures for the registration and deregistration of network users have been established to ensure that all users' access rights match their authorisations. These procedures are detailed in the ICT User Management Procedure[2]; this should be used in conjunction with the Network Registration Form and Acceptable Use Policy. All business system user access rights will be reviewed at regular intervals by the system owner or other staff as defined in the User Management Procedure to help safeguard against potential security breaches.

[2] Copy available on the College Intranet

Disposal of Data

The College will ensure that when permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site. Damaged storage devices containing sensitive data will also undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded.

Ownership, Storage and Archiving of Information

College information that is deemed confidential, or is classed as personal data or sensitive personal data under the Data Protection Policy cannot be stored on or transferred to any unauthorised and non-encrypted storage device or media (eg. USB, personal laptop or College laptop without encryption software). Only the Head of ICT and Information Records and Projects Manager can authorise the use of a device for this purpose.

All information assets are owned by the College and a System Owner and Data Owner will be in charge of each ICT system holding information or records. This individual will be named on the Information Asset Register.

The College will ensure that appropriate backup and system recovery procedures[3] are in place before any archiving of data can commence. The College will also ensure that day-to-day information is stored efficiently and is readily available to authorised users.

Where storage is allocated to system or share owners directly the data held will be managed by the system or share owner.

Storage media used for the archiving of information must be appropriate to its expected longevity and the format in which the data is stored will be carefully considered, especially where proprietary formats are involved.

Use of USB storage will not be permitted by staff unless the USB is encrypted. ICT Services will implement a process for encrypting these.

Access to Records

All information used for, or by the College, will be filed appropriately and according to its classification. Paper copies of sensitive or classified material will be handled in accordance with the College Records Management Policy.

[3] Part of the ICT Business Continuity Plan, available from the ICT Department

B. BUSINESS CONTINUITY POLICY

B1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding business continuity in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. processes used for assessing and addressing risks to business continuity are clearly defined;
b. responsibilities for preparing and implementing business continuity plans are suitably delegated;
c. IT related systems are categorised appropriately within the College, based on designated levels of criticality;
d. appropriate business continuity plans for critical IT systems are produced in a logical and robust manner;
e. interruptions to business systems are suitably neutralised;
f. vital IT services and systems are protected from major failures or disasters.

B2. Guidance

Business Impact Analysis

The ICT department Business Impact Analysis[4] provides information on organisational risks relevant to ICT operations and contains plans for mitigation. It also includes a staff recovery profile.

Business Continuity Planning

The ICT department Business Continuity Plan[5] covers operational procedures for the recovery of all business dependent IT systems within the College. It also cross references key documentation and information sources.

[4] This document is not externally published
[5] Full version is not published but may be available from ICT on request

C. SOFTWARE MANAGEMENT POLICY

C1. Objectives and Scope of the Policy

This Policy applies to all users and owners of College IT related information systems and sets out College policy regarding the management of software in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. all software installations within the College are controlled in a secure and legitimate manner;
b. only authorised individuals will perform software updates;
c. risks to information and information systems are minimised;
d. systems are protected against malicious threats posed by viruses, ransomware and worms
e. appropriate procedures are in place regarding the maintenance of software within the College.

C2. Guidance

Business Applications

College business applications will be managed by suitably trained and qualified staff, trained in relevant information security issues.

Software Implementation

The College will ensure that procurement or implementation of new or upgraded software is carefully planned. Information security risks associated with such projects will be mitigated using a combination of procedural and technical controls.

To prevent copyright infringements and protect all information systems, the College will run regular audits and closely monitor all software renewals.

Software **must not** be installed onto any PC within the College by unauthorised staff or students and anyone caught doing so may face disciplinary proceedings.

Business Requirements

Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

Vendor Supplied Software

The College discourages any modifications to vendor-supplied software. Only strictly controlled essential changes shall be permitted and the development of interfacing software, will be tested before changes are moved to the live environment.

Software Patching and Updates

System Owners are responsible for arranging with ICT the update and patching of applications and dependent software such as Java, Flash etc. deployed throughout the college.

For the College's procedures on patching please see appendix C.

D OPERATIONS POLICY

D1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the operation of key systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. College information processing systems are used and managed in accordance with best practice initiatives regarding the protection of information security;
b. changes to operational procedures involving business critical or sensitive information, will be analysed and all associated risks will be assessed to ensure that the needs of information security have been addressed;
c. the implementation of any College IT systems will be properly managed in a secure and robust manner.

D2. Guidance

Physical Security and Access Control

Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. College staff with authorisation to enter such areas will be provided with information on the potential security risks and the measures used to control them.

Operation of IT Systems

The procedures for the operation and administration of College business systems will be appropriately documented, with all such procedures and documents being regularly maintained and reviewed by the System Owner.

Security Incidents

The reporting of security incidents and suspected security weaknesses in College business systems should be recorded via the ICT helpdesk.

Software Faults

The reporting of software malfunctions and faults in College information processing systems will be made via the ICT Helpdesk. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

System Development and Testing

New systems and upgrades are accepted for use subject to testing. Suitable testing of the system will be carried out by system owners prior to migration to operational status.

In collaboration with the third party vendor, processes will be established by the System Owner to control the maintenance and development of all operational software.

Security Risks

Security risks to the information assets of all system development projects shall be assessed by the relevant Project Manager or System/Data Owner and access to those assets shall be controlled.

E. SYSTEM MANAGEMENT POLICY

E1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the management of IT systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. the management of College computer systems is appropriately structured and relevant responsibilities and required behaviours are suitably identified;
b. all software and services will be managed and maintained in a clear and precise manner.

E2. Guidance

Staff Training

College systems are managed by suitably trained and qualified staff. All system management staff shall be given relevant training in information security issues.

Access Controls and Services

Access controls shall be maintained at appropriate levels for all College systems by ensuring that users are granted appropriate access rights to systems. This is also supported by the College Network Registration Form, Acceptable Use Policy and ICT User Management Procedure[6]. Any change of access permissions must be authorised either by the System Owner or another appropriately authorised person or committee.

Access to all information services will be via a secure log-on process. All access to information services is to be logged and monitored by the College to identify potential misuse of systems or information.

The Information Access Policy provides the relevant guidelines regarding the use of passwords within the College.

System Security

Access to system commands is to be restricted to those persons who are authorised to perform systems administration or management functions.

The implementation of new or upgraded software must be carefully planned and managed.

[6] Copy available on the College Intranet

System Capacity

The capacity demands of systems supporting business processes will be monitored by System Owners and various projections of future capacity requirements made to ensure that appropriate processing power, storage and network capacity is available when required.

F. SYSTEM PLANNING POLICY

F1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the planning of IT systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. information systems within the College are appropriately specified and designed;
b. any requirements or risks associated with College information systems will be suitably identified and risk assessed;
c. information systems will be specifically designed and configured to enable appropriate security safeguards to be implemented.

F2. Guidance

System Authorisation

New information systems, or enhancements to existing systems, must be authorised via the Information Management Steering Group. The proposals and business requirements for all authorised systems must specify requirements for security controls. Where Personal Data is to be held, a Data Protection Impact Assessment must be completed. The Data Protection Impact Assessment must be reviewed by the Data Protection Officer as detailed in the Data Protection Policy.

System Implementation

The implementation of new or upgraded systems must be carefully planned and managed, by the relevant Project Manager or System Owner, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

All systems should be maintained in accordance with the manufacturer's recommendations.

Information Assets

Information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the Records Management Policy, Software Management Policy and Business Continuity Plan[7]. The details should be held in the Information Asset Register. A risk assessment will also be undertaken to identify the probability and impact of security failure.

[7] Full version not published but may be available from ICT on request

Equipment

Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment supporting business systems shall be correctly maintained and given adequate protection from unauthorised access, environmental hazards and electrical power failures.

Access Controls

Access controls for all information and information systems are to be set at appropriate levels in accordance with the Information Access Policy.

Access to operating system commands and application system functions is to be restricted to those persons who are authorised to perform systems administration or management functions.

G. REMOTE ACCESS POLICY

G1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the remote accessibility of networks and systems, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. security of College information assets is maintained when working with mobile devices;
b. College information assets are accessed from a mobile device in ways that are compliant with information security policies;
c. the benefits of teleworking can be achieved without unduly increasing the risk to information assets.

G2. Guidance

Remote VDI Access

The supported methodology for providing access to the College ICT network and systems from anywhere outside the College to authorised users is the College Virtual Desktop infrastructure (VDi). The procedures for authorised users to access the VDi is published on the College Web site via the MyNewCollegeDurham link.

Mobile Computing

The College will seek to protect mobile computing equipment against unauthorised access and register devices appropriately to monitor ownership and location.

Users borrowing laptops, phones and any other mobile computing equipment from the College will do so according to this policy and the ICT Equipment Loans Policy and Procedures[8].

Mobile Computing Guidelines[9] are available for users.

[8] Copy available on the College Intranet
[9] Various manuals are available from the ICT Department Intranet pages

H NETWORK MANAGEMENT POLICY

H1. Objectives and Scope of the Policy

This Policy applies to all users of College IT related information systems and sets out College policy regarding the management of the College network, in accordance with legislation and best practice initiatives.

The Policy objectives are to ensure that:

a. the College adopts a continuing risk assessment approach to network management;
b. appropriate technical and procedural controls are in place to reduce the impact of potential network risks;
c. emergency measures are in place to deal with faults and incidents relating to the College network.

H2. Guidance

Network Supervision

The College network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff shall be aware of information security issues.

Network Performance

The network will be designed and configured to deliver high performance and reliability to meet College needs whilst providing a high degree of access control and a range of privilege restrictions.

Network Protection

The network will be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting College business systems.

Wireless access will be supported by appropriately configured SSIDs.

Devices attempting to connect with the network via wifi will be assessed to ensure they meet current security standards. If this is not the case they will be prevented from connecting. The ICT Operations Manager will determine the level of security standard[10].

External devices

All users are responsible for the maintenance of any personal device connected to the network. Where possible devices should be set up to receive updates

[10] Bradford Network Sentry Campus manager is deployed to decrease the risk of rogue equipment being attached to the College network.

automatically. Where automatic patching is not available, device owners should ensure manual checks occur on a regular basis to ensure the device is up-to-date.

Network Resources

Access to the resources on the network will be strictly controlled to prevent unauthorised access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

Network Authentication

Any user who requires access to the College network will need to complete the appropriate registration forms in accordance with the Acceptable Use Policy.

Change Control Procedures

The implementation of new or upgraded software or firmware must be carefully planned and managed. All changes must be properly tested and authorised before moving to the live environment.

Network Access Points

Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them. These are subject to controlled access.

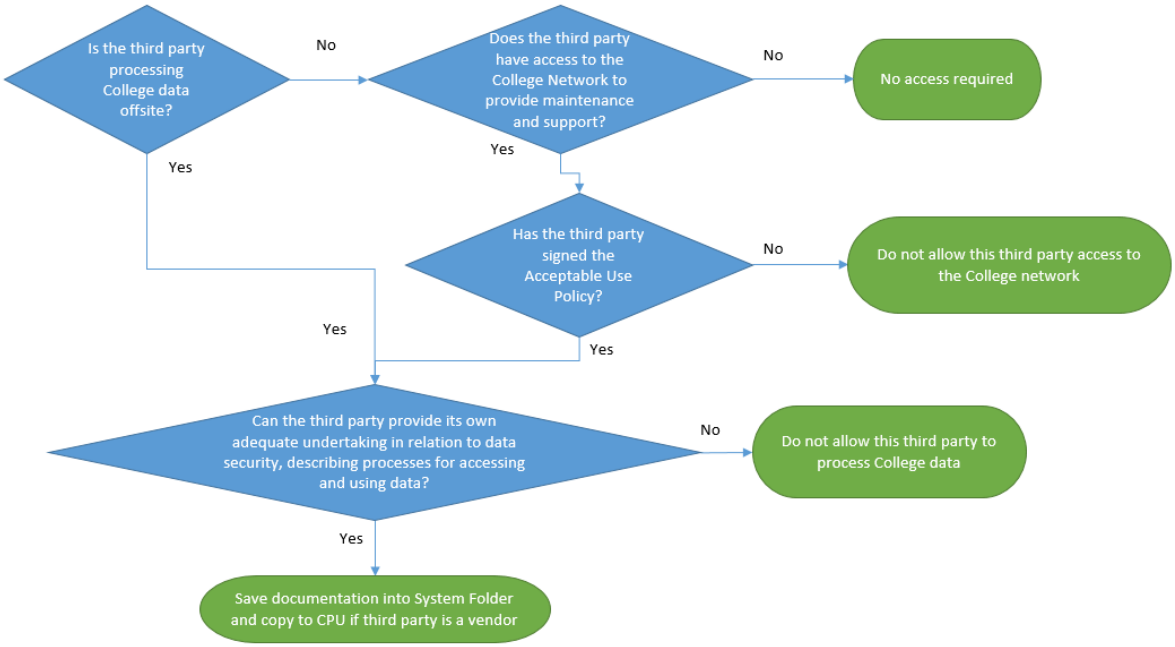
Network Attacks

Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

Appendix A: Information Security Checklist

1	Describe the platform on which our data will be held	[Please complete]
2	Is the system regularly patched in accordance with the platform guidance?	[Please complete]
3	Is your datacentre protected by a Firewall, anti-virus and intrusion detection?	[Please complete]
4	What are your backup and restore procedures?	[Please complete]
5	Is your datacentre segregated to prevent other hosted organisations accessing our data?	[Please complete]
6	Describe the physical location where our data will be held, including in which country this will be.	[Please complete]
7	What physical security is there at this location protecting the facility, datacentre and servers from unauthorised access?	[Please complete]
8	Do you have any security accreditation (eg. ISO27001)?	[Please complete]

Appendix B: Third Party Access



Appendix C: Procedures for Patching

1. Patching

a. General

Devices that connect to the College network must be protected from vulnerabilities that exist within the Operating System. Security patches must be installed within a reasonable timeframe from their release but only after testing. In exceptional circumstances, it may be required to apply any deemed critical patches immediately to protect against any serious vulnerabilities.

b. Microsoft platforms

Patching will be managed and performed by ICT team using Microsoft SCCM Patch Manager and will cover Microsoft Servers, both physical and virtual, all physical desktops, laptops and Surface Pros. Microsoft SCCM will not cover the Virtual Desktop estate.

Microsoft DMZ servers are not updated by SCCM and are manually updated every month by a member of the IT team. A list of DMZ servers are available upon demand.

The VDI team patches VDI Gold images at the end of the month and the desktops are redeployed.

c. VMWare ESX estate

VMWare ESX is used by ICT for virtual server and Virtual Desktops. These systems use the built-in Update Manager to download and manage the patches required for the hosts.

These systems are patched out of term to minimise disruption to students however it may be required to apply any deemed critical patches immediately to protect against any serious vulnerabilities. This can be done on a host-by-host basis until the environments are fully patched.

d. Wireless

The Wireless system will be patched out of term to minimise disruption to students however it may be required to apply any deemed critical patches immediately to protect against any serious vulnerabilities. The Ruckus controller automatically deploys new firmware to the Access Points.

e. Firewalls

The College has two sets of Firewalls, Juniper SRXs for SonicWALL firewalls. SonicWALL's are updated as and when prompted by the Firewalls themselves and at a convenient time.

SRX firewalls are updated once a year out of term to minimise disruption. However, any patches deemed critical will be patched as soon as is possible.

f. Routers

The College has no routers under its direct control. All routers are managed by third party suppliers.

g. Switches

The College uses Extreme hardware throughout the college and takes guidance from its Network support company about what patch level the switches should be. All possible implications are reviewed before deployment, as any negative impact could be substantial.

Any patching takes place out of term time to minimise disruption.

h. Test patching

A test-patching group has been configured to cover various servers and PCs that cover, but not restricted to, SQL, Exchange, file servers and Lync systems. The test group patches are deployed on the last day of the month and results and effects of the patching are analysed by ICT prior to deployment on the rest of the College estate.

Following the test patch results if any test systems display any issues, then the patches for the affected systems are withheld for wider distribution. Otherwise, full patching will take place 7 days after the test group has been deployed.