SPARSHOLT COLLEGE HAMPSHIRE

ANDOVER COLLEGE prepared for life

IT Policy

Integrity, Sustainability

CULTIVA Sustainable Learning Solutions

matrix

Landex

TRAINING QUALITY STANDARD

With excellence in

Environmental and Land Based Training

Recognising the best organisations for training and development solutions

Principal: Tim Jackson BTech (Hons), PGCE

Our Mission

To inspire learners to recognise and achieve their full potential

Our Values

Excellence, Passion, Team Work, Integrity, Innovation,

Sustainability, Valuing Others and Supportiveness

Sparsholt College Hampshire, incorporating Andover College

The *IT Policy* was approved by the Board of Governors in October 2017. It supercedes all previous versions and is effective from October 2017

Equality Impact Assessment	Conducted: September 2017
Originator: IT Manager	Located: College Intranet
Date of next scheduled review: September 2019	

IT Policy

Integrity, Sustainability

Table of Contents

SPARSHOLT COLLEGE HAMPSHIRE incorporating ANDOVER COLLEGE

IT Policy

Integrity, Sustainability

1 Introduction

This policy defines a framework which protects the College's computer systems, assets, infrastructure and computing environment from threats, whether internal, external, deliberate or accidental.

For the purposes of this document the following terms apply:

- We/Our/Us – Sparsholt College incorporating Andover College
- You – the end user, the reader of this policy
- IT – Information Technology, including physical hardware, software and provided services
- ITS – the IT Services Department
- Intranet – Internal Web based information supplied via browser
- SLT – the Strategic Leadership Team

Ignorance of this policy and the responsibilities placed on you is not an excuse in any situation where it is assessed that you have breached the terms set.

Students are directed to an abbreviated version of this document (Section 18 – IT Acceptable Use) during their registration each year and are required to acknowledge their agreed adherence to and compliance with the policy. A copy of the abbreviated version is also shared with all new staff during their IT induction.

Staff are advised of this document during their induction and of the College's requirement for them to adhere to the conditions therein. Staff are expected to refresh their knowledge of the policy periodically to keep abreast of changes. An up-to-date version can be found on the Policies page of the Intranet (Sharepoint).

2 Applicability

This policy applies to:

- Students
- Staff
- Visitors
- Guests
- Contractors
- Partners and Affiliates of the College

You are responsible for ensuring anyone within your area of responsibility is complying with this policy.

3 Key Principles

All IT systems and information contained within them will be protected against unauthorised access.

All use of our IT facilities will comply with this Policy.

Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy our expectations that such assets will be managed in a professional, safe and dependable manner.

All employees of the College are required to familiarise themselves with this policy and comply with its requirements.

Managers have a responsibility for ensuring adherence to and compliance with this policy throughout their areas of responsibility.

The integrity of all IT systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of ITS.

All regulatory and legislative requirements regarding computer security and IT based information, confidentiality and integrity will be addressed by ITS.

All breaches of security will be reported to and initially investigated by ITS.

All users have a responsibility to report promptly to ITS, any incidents which may have an IT security implication for the College.

4 The IT Environment

ITS manages, maintains and operates a range of IT equipment including, but not limited to, Servers, Switches, Routers, Firewalls, Backup Systems and the overall Network Infrastructure interconnecting these systems.

The IT environment is defined as all IT resources, Software, Data, Physical and Network Infrastructure managed and overseen by ITS and all devices that can physically connect to it, and that have been authorised to connect to it. This policy covers the entire IT environment.

All connections to the College infrastructure, be they temporary or permanent, via our physical network, wireless network, or remote working connections, are similarly subject to the conditions of this policy.

IT resources not owned by us, may be connected to our network. However, all such resources must comply with our guidance governing the use of IT resources.

IT reserves the right to monitor, log, collect and analyse the content of all transmissions on our networks at any time deemed necessary for performance, fault diagnostic and compliance purposes.

5 Physical Safety

All IT is supplied in a working state. Visual inspections of all IT equipment should be carried out before use; any equipment found not to be working, or suspected of being faulty or damaged, should be reported immediately to the ITS Service Desk.

Open drinks containers, cups, beakers, etc. should not be within 1 metre of any IT equipment.

6 IT Security

In order to ensure the security of the College IT estate, IT Services will:

- restrict and monitor physical access to data centres
- run a Mobile Device Management Suite in order to be able to track and trace the location of the majority of mobile devices (this also gives the ability to wipe devices remotely should they become compromised)
- use devices or mechanisms for securing and protecting IT equipment main components and contents from theft
- enforce use of a log-on or power-on password on portable IT equipment wherever possible

In order to ensure the security of the College IT estate, staff are expected to:

- where practical, lock doors of offices containing IT equipment when left unattended and outside of general office hours
- physically secure any unattended portable IT equipment - for example locked in an office or a desk drawer
- hide any portable equipment from view when being transported in a vehicle, and remove it when the vehicle is unoccupied e.g. overnight

Removable media, USB memory sticks etc, must not be used to store any personal information. Staff should contact IT Services for advice if they feel they have a requirement to do so.

Staff must not store personal information on personally owned portable equipment. Please contact the IT Manager or the Director of Information & Funding for advice if required.

7 Provision of IT Equipment

IT equipment is supplied on receipt of requests from HOF's or Managers with approval from their appropriate SLT member.

Academic staff

- Full Time – Issued with appropriate portable device
- Part Time > .4 fte – Issued with appropriate portable device
- Part Time < .4 fte – To use portable device from departmental pool
- Sessional / Casual – To use portable device from departmental pool

Any staff that work on both campus locations or carry out an ‘on-the-road’ post, a mobile device and dock can be supplied if practical.

Any staff where an appropriate portable device would make a marked positive impact on their ability to work can be issued with such a device where approved by their Manager and SLT member subject to budgetary constraints.

Where IT equipment is positioned and installed by IT Services it is not to be moved without IT Services assistance and approval.

Damage to any IT equipment must be reported to the IT Service Desk at the earliest opportunity.

IT Services will maintain a register of portable equipment that is issued to staff, and staff will sign for all such equipment.

At the end of your employment all College assets, including any peripherals, must be returned in good working order, and signed back in to IT Services.

8 Data Security

All use and processing of personal information and data is governed by the auspices of the Data Protection Act 1998. On 25th May 2018, the Data Protection Act is scheduled to be replaced by the General Data Protection Regulation (GDPR), at which point governance of use and processing will transfer. Staff are reminded of their responsibilities under the Act and the future GDPR in maintaining the security and preventing the unauthorised disclosure of any personal data held.

In order to ensure the security of personal information, IT Services will:

- enforce a minimum of 128-bit encryption on portable devices
- prevent users from storing data on local drives of non-portable IT hardware
- require a change of network password for staff every 90 days
- wipe hard drives and memory of all equipment before disposal

In order to ensure the security of personal information, staff are expected to:

- lock their IT device using **-L** or **[Ctrl]-[Alt]-[Delete]**, then **[Enter]** when leaving their PC/Surface/Laptop unattended
- keep their passwords secret
- avoid opening emails on a projected screen – private information may be displayed to anyone else in the room or even outside via the window
- when emailing personal data, password protect in an attachment and phone the password through to a trusted number
- refer all requests for disclosure of personal data from external sources to be dealt with via the central register
- contact the Director of Information and Funding if in doubt about any data security matter
- only use College approved cloud based repositories (OneDrive for Business and SharePoint Online, accessed via their College email address)
- check the email addresses of intended recipients before sending any email, as email programs often incorrectly predict email addresses you are typing in
- consider using BCC to restrict visibility of other recipients' addresses when emailing to a group of recipients (especially where there are large numbers of recipients or some external addresses).

9 Loss or Theft of Confidential Information

All incidences of loss or theft of confidential information must be reported immediately to the College's Data Controller (the Director of Information and Funding). A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords, to the loss or theft of confidential information either inside or outside the College.

A security incident is any event that has resulted or could result in:

- The disclosure of personal/sensitive/confidential information to any unauthorised person.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.
- Adverse impact, e.g. Negative impact on the reputation of the College.
- Threat to personal safety or privacy.
- Legal obligation or penalty.
- Financial loss or disruption of activities.

All incidents must be reported to the Data Controller in the first instance, as soon as possible after the event.

In the case of a serious potential breach, the Data Controller will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies or other third parties, e.g. insurers. The Data Controller will retain a central register of all such incidents occurring within the College.

The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, you should consult the Data Controller who will decide what action should be taken.

Examples of breach of security:

- Loss of computer equipment due to crime or carelessness.
- Loss of portable media devices (memory sticks etc.) containing personal data.
- Accessing any part of a database using someone else's password.
- Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

Examples of a breach of confidentiality:

- Finding confidential/personal information either in hard copy or on a portable media device outside College premises or in any of the College's unsecured common areas.
- Finding any records about a staff member, student, or applicant in any location outside the College's premises.
- Passing information to unauthorised people either verbally, in writing or electronically.

10 Account Security

Access to our IT systems is via a Username and secure password. It is your responsibility to keep your password secure. ITS cannot see your password but can, on request, reset it for you either by request in person to the service desk with your college ID, or by having your manager (in the case of staff members) or lecturer/tutor (in the case of students) send a request via email.

Passwords must be

- Minimum 8 characters long.
- Contain at least 3 character sets (uppercase letters, lowercase letters, numbers, special characters).
- Not contain your username.

- Changed every 90 days for staff.
- Not be the same as your last 8 passwords.

HR, or an appropriate delegate, must provide written confirmation to ITS to allow us to grant access to a staff account in the event of leave or sickness and where required for the operation of the college.

HR must provide written confirmation to the IT Manager to suspend, cease or reset the password of a staff account in the event of an investigation.

Staff IT accounts will be created and suspended on the dates published in the starters and leavers list as provided by HR, unless specifically requested by the appropriate manager to the IT Manager. However, as part of the College's safeguarding process no IT account for staff/agency staff/self-employed/contractors will be set up unless permission is given by the HR department.

Student IT accounts are created automatically after the student is enrolled on ProSolution. Student accounts are disabled within 24 hours of the student being withdrawn from all courses on ProSolution, or on the 90th day after their course completion date. 30 days after student accounts are disabled, the related OneDrive and email accounts are deleted in order to free up licences.

11 Email

Email is not a completely secure medium. You should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context, that once an email is sent you cannot control what the recipients might do with it, and that it is very easy to forward large amounts of information.

Similarly you should not necessarily trust what you receive in an email - in particular, you must never respond to an email request to give a username or password. Any such emails should be referred to ITS.

You need to be aware that any messages deemed to bring the College's name into disrepute will be treated and investigated as a disciplinary matter.

Your college email can be retrieved on your own personal device but in doing so your device has to comply with this IT policy, and in the process we will be granted specific rights on your device - consult your device manufacturer for exact details. Instructions for doing so can be sought from the IT Service Desk.

12 File Storage

You have access to and on campus, centrally managed file storage facility via personal and shared drives.

Personal Home drive storage, sometimes referred to as the 'Z Drive', is limited to 3GB for staff users and nominally 250MB for Students. OneDrive for Business storage for all users is set to 1TB.

Personal/home drive storage should only be used for your personal data and data that no-one else has a requirement to access.

Shared/departmental storage should be used for all other storage.

Access rights to all data is maintained by ITS to guidance from the data owners or SLT.

Use of any cloud-based file storage other than OneDrive for Business, as provided by us, is strictly forbidden. Any use of such breaches our policy on safeguarding information.

The use of removable media in the form of memory sticks as the sole location for storing data is strongly discouraged. Data loss through physical loss or corruption of data is commonplace on such items. Personal/sensitive data must not be stored on such media.

13 The Internet

You should consider the security implications of any information you put on our Website or Virtual Learning Environment, and we reserve the right to remove any material which we deem to be inappropriate, illegal or offensive.

You should not in any way use any areas of our Website for commercial purposes not related to the College's business.

You shall not in any way use web space to publish material which undermines IT security at the College. In particular this covers making information available about how IT security is implemented at a practical level, or any known weaknesses.

Any use of the internet will also comply with the College's Social Media Policy.

We reserve the right, without warning, to block access to external web services, where we deem it appropriate.

14 Campus Network

You must seek permission from ITS before physically connecting any form of IT device to the physical College network.

Any device connected to our IT network can be removed without warning for breaching the IT policy.

All network traffic may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised personnel, are kept for no longer than necessary and in line with current data protection guidance.

Such records and information are sometimes required - under law - by external agencies and authorities. The Data Controller will comply with such requests on behalf of the College when formally submitted.

The only protocol family supported by IT Services is TCP/IP. You must not run or allow to be run:

- DHCP servers
- DNS Servers
- Routing Protocols (such as OSPF, RIP etc)
- Network Discovery Protocols
- Internet Connection Sharing
- Port Scanners

Neither are you permitted to:

- Attempt DDNS dynamic Name Server Updates.
- Set up network file shares that are writable without a password.
- Re-distribute network access to others, nor any College resource made available to them.
- Configure any device attached to the Network with any IP address not specifically allocated to them.
- Connect any form of Wireless Access point to the Network, nor configure any computer with wireless capability such that the Network can be accessed wirelessly.
- Download or distribute copyright material in breach of any licence conditions.
- Run Peer to Peer applications that distribute copyright material.
- Use proxy services to circumvent network security.

15 Remote Access to Systems

Remote access is defined as accessing systems from a physically separate network. This may include:

- Direct connections across the Internet.
- VPN (Virtual Private Network) connection
- VDI (Virtual Desktop Infrastructure) Connection.

Any user with a valid College IT account may access systems as appropriate. Remote access is allowed via secure methods only.

Remote connections to any campus IT service is subject to the same rules and regulations, policies and practices just as if they were physically on the campus. IT Services provide the only VPN/VDI service that may be used.

All connections via these services will be logged. No other remote access service shall be installed or set up, including single modems connected to servers or workstations. Any active dial-in services found to be in existence will be removed from the network.

16 Anti-Virus Security

When connected to our IT network, you must ensure that you are running with adequate and up-to-date anti-virus software at all times. If you suspect viral or malware infection on your machine, a complete security scan should be performed. Should IT Services detect a device behaving abnormally due to a possible infection it will be disconnected from the network until deemed safe. Reconnection will usually only be after direct liaison with IT Services.

17 Related Documentation

College HR Regulations
College Acceptable Use Policy
General Guidelines

18 IT Acceptable Use

18.1 Introduction

This is a summary of the IT Policy specifically aimed at non-Staff members.

18.2 General

When using our IT services you must at all times comply with the law.

When using our IT services you must **NOT**:

- Interfere with any others' use of these facilities and services
- Use a computer that you have not been authorised to use.
- Access any programme or data which has not been specifically authorised for your use.
- Use or copy any data or programme belonging to other users without their express and specific permission.
- Alter computer material belonging to another user without the user's permission.
- Use our computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- Use our computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for academic purposes which would require the fullest disclosure and special authorisations.)
- Use our computing services to conduct any form of commercial activity without express permission.
- Use our computing services to disseminate mass (unsolicited) mailings.
- Install, use or distribute software for which you do not have a licence.
- Use the IT account of another member of college staff or another student.

And remember

- The College owns all intellectual property / capital / connect in perpetuity that is produced and stored on College computing services assets.
- The College reserves the right to access your College account with permission from the HR Manager / Head of Department / Faculty or SLT member.
- In general, use of College computing services should be for your study, research, teaching or the administrative purposes of the College. Modest use of the facilities and services for personal use is accepted so long as such activity does not contravene the conditions of this policy.
- Use of College computing services for your own commercial work may be governed by software licence constraints and users should verify with IT Services Staff that the intended use is permissible under the terms of those licences.

- If you think your account has been compromised change the password and contact the IT Service Desk for advice.

18.3 Authentication

Access to the secure areas of the network is controlled by Username and password; these are issued at either contract start or course start. Accounts will be disabled within a reasonable time of contract end or course completion. Account security is paramount to system security - **never give your password to anyone**.

Staff usernames are first initial & Surname e.g. Joe Bloggs – jbloggs

Student usernames are the student ID numbers only e.g. ABC12345678 - 12345678

Staff Passwords must:

- Be a minimum of 8 characters long.
- Contain at least 3 character sets (uppercase, lowercase, numeric, special).
- Not contain the Username.
- Not be the same as the last 8 passwords.
- Be changed every 90 days.

Student passwords must:

- Be a minimum of 6 characters long.
- Contain at least 3 character sets (Uppercase, Lowercase, Numeric, Special).
- Not contain the Username.
- Not be the same as the last 8 passwords.
- Be changed once a year.

18.4 Data Storage

Files can be saved to the provided drives; limited space is available so be aware of space constraints and save to shared areas where possible.

Space is provided for each user on a Personal / Home / Z drive. Files that cannot be stored in shared areas can be stored here.

- Students – 250Mb
- Staff – 3Gb

Use of any cloud based file storage other than OneDrive, as provided by us, is strictly forbidden. Any use of such, breaches our policy on safeguarding information.

The use of USB memory sticks is discouraged - they break and lose data very easily.

18.5 Email

Email is provided for all staff and students.

18.6 Personal IT equipment

18.6.1 Anti-Virus

When connected to our IT network, you must ensure that you are running with adequate and up-to-date anti-virus software at all times. If ITS detect a device behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe.

18.6.2 Remote Connections

Any user with a valid College IT account may access systems as appropriate. Remote access is only allowed via the secure methods we supply.

Remote connections to any campus IT services are subject to the same rules and regulations, policies and practices as if they were physically on the campus. All remote connection attempts will be logged.

18.7 Monitoring & Logging

All activities can and will be monitored and logged from time to time for security, diagnostic and account / audit reasons. Logs are only available to authorised individuals and retained for no longer than necessary.

Such records and information are sometimes required - under law - by external agencies and authorities. We will comply with such requests when formally submitted.

When using portable IT equipment we have the ability to monitor and record its, and therefore your, physical location.