The Talentum Learning Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	July 2017	Review date:	**May 2019**
Policy Owner:	Trust Board	Page: 1 of 36			
Audience:	Trustees ☑	Staff ☑		Local Governing Bodies ☑	
	Parents ☒	Pupils ☒		General Public ☒	

Information and ICT Security Policy

In this policy document, 'The Talentum Learning Trust', 'Learning Trust', 'the Trust' or 'TTLT' should be interpreted to include one or all of, but not limited to, the following establishments:
Churnet View Middle School,
Leek High School,
Westwood College.

Version control

Version	Author	Date of amendment
1.0	SCC Information Security	11-MAR-2011
2.0	Duncan V. Smith	24-FEB-2012
3.0	Duncan V. Smith	10-FEB-2014
4.0	Duncan V. Smith	04-MAY-2016
5.0	Duncan V. Smith	03-JUL-2017
6.0	Duncan V. Smith	13-SEP-2017
7.0	Clarissa A. Williams	18-SEP-2017
8.0	Duncan V. Smith	01-MAY-2018
8.1	Duncan V. Smith	06-JUN-2018

1. Contents

Policy Statement

The objective of this Information Security Policy is to protect the information assets processed by The Talentum Learning Trust from all appropriate threats. Compliance with this Information Security Policy is necessary to ensure the confidentiality, availability and integrity of the Trust's data, and minimise information security incidents.

In support of this Information Security Policy the Executive Headteacher, Headteachers, Directors and Local Governors accept their role in being fully accountable for information security and are committed to:

- Treating information security as a high priority
- Creating a security aware education environment
- Implementing controls that are proportionate to risk
- Promoting individual accountability for compliance with information security policies and supporting procedures and guidance

This document is written for all staff in schools within the Talentum Learning Trust, although some of the information contained will be relevant to students or Guests/3rd Parties.

Scope

Information takes many forms.
The scope of this Information Security Policy includes, but is not limited to:

- All information processed by the Trust electronically or in paper form, including but not limited to:
    - Pupil data and external partner information and reports
    - Operational plans, accounting records and minutes
    - Employee records
- All information processing facilities used in support of the Trust's operational activities to store, process and transmit information
- All external parties that provide services to the Talentum Learning Trust in respect of information processing facilities

Policy Coverage

This Information Security Policy provides that the Talentum Learning Trust shall ensure that:

- Information shall be protected against unauthorised access
- Information shall be protected against unauthorised disclosure
- Integrity of information shall be maintained
- Information shall be available to authorised users when required
- Statutory and legal obligations shall be met
- Unauthorised use of information assets and information processing facilities shall be prohibited
- Students shall continually be made aware of information security, it's importance to them and how it can impact on their time in school
- Any third parties utilising the Talentum Learning Trust sites or facilities are aware of their responsibilities under this policy
- All breaches of information security, actual or suspected, shall be reported and investigated.
- Controls shall be commensurate with the risks faced by Talentum Learning Trust
- This information security policy shall be communicated to all employees for whom information security training shall be regularly given

In support of this Information Security Policy, more detailed security guidance and processes shall be developed for employees, information assets and information processing facilities.

The guidance documents associated with this policy will cover Information Security in schools in the following areas:

- Internet and Email Usage
- Technical Security

Responsibilities

The Executive Headteacher, Headteachers, Directors and Local Governors of The Talentum Learning Trust shall be accountable for ensuring that appropriate security and legal controls are identified, implemented and maintained. They shall be supported in this task by all employees. Students need to be made aware of their responsibilities under this policy, and supported to uphold it.

The Executive Headteacher, Headteachers, Directors and Local Governors shall appoint staff member(s) who shall be responsible for managing information security at an operational level.

It is the responsibility of all school employees, students and 3rd parties to adhere to school policies.

Non-compliance of the Information Security Policy by any employee shall result in disciplinary action. Non-compliance by 3rd parties shall result in their connection being terminated.

The Executive Headteacher, Headteachers and Directors must approve this Information Security Policy.

Policy Implementation

The Executive Headteacher, Headteachers, Directors and Local Governors along with the operational manager(s) with responsibility for Information Security at Talentum Learning Trust establishments must implement such Information Security controls as they see fit for their establishment.

Policy review and maintenance

This Information Security Policy shall be reviewed annually by the Executive Headteacher, Headteachers and Directors or at other times as dictated by operational needs.

2. Email

This Email section of the policy shall apply to all email messages processed by The Talentum Learning Trust teachers, administrative staff and students.

All teachers, administrative staff and students shall remember that standard email is not a secure form of communication. The messages that you send may be over networks owned by other people. A more secure method of communication shall be used, if the content of an email is sensitive or critical such that if the contents were disclosed or modified by an unauthorised person it could cause embarrassment, distress or financial loss.

Internet access refers to the use of any resources from the World Wide Web, whether browsed or downloaded.

Policy Statements

- The Talentum Learning Trust's email facilities shall be used in accordance with:
    - Specified and published policies and guidance including e-safety.
    - All appropriate legislation

- Internet and Email usage shall be monitored to ensure compliance with policies and guidance

- This Internet and Email Policy is approved by, and has the full support of the Executive Headteacher and Directors.

- The Executive Headteacher and Directors shall ensure that employees and students receive continual education and training to support compliance with this internet and email policy and the Trust's e-safety policy.

- The Systems Manager(s) shall develop, maintain and publish processes to achieve compliance with this Internet and Email Policy.

- All teachers and administrative staff shall be responsible for implementing this Internet and Email Policy in their areas of responsibility.

- All employees and students provided with internet and email facilities shall sign the Acceptable Use Policy to indicate their agreement to comply with this policy.
  This can be via written or electronic means.

Email Usage Principles

In this policy document, 'The Talentum Learning Trust', or 'Learning Trust', or the 'Trust' should be interpreted to include one or all of the following establishments: Churnet View Middle School, Leek High School, or Westwood College.

The use of the Learning Trust email facilities shall indicate acceptance of this Email Policy.

The Talentum Learning Trust provides email to assist employees in the performance of their jobs, and students with their learning objectives. Whilst its use should be primarily for official Trust business, incidental and occasional personal use of email shall be permitted, on the understanding that:

- Personal messages shall be treated the same as any other message

- Personal use of the email system shall never impact on the normal traffic flow of business related email
- The Talentum Learning Trust shall reserve the right to purge identifiable personal email to preserve the integrity of the email systems.

No employee or student shall send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Unwelcome propositions
- Profanity, obscenity, slander or libel
- Ethnic, religious or racial slurs
- Political beliefs or commentary
- Any message which could be viewed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

The Talentum Learning Trust owns the e-mail system which means that all email traffic, both sent and received, including attachments, shall be monitored and reviewed and any action deemed appropriate shall be taken.

This means that nothing should be taken to be private, even if marked as “private” and/or “confidential” or with any similar wording.

This monitoring will make sure that this policy is effective and that users of the email system are abiding by its content. The monitoring is also to ensure that the Talentum Learning Trust email system(s) are working properly.

All teaching staff, administrative staff and students shall ensure compliance with relevant legislation.

Email folders shall be reviewed regularly and any non-essential messages shall be deleted.

- A standard footer should be appended to all external email messages:
  Limiting liability and including an appropriate disclaimer
  Detailing the Learning Trust establishment’s registered address

- Internal email and other internal information shall not be forwarded to destinations outside of the Learning Trust domain(s) without the authority of the appropriate individual.

- Email users shall not forward chain letters either internally or externally. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Virus warnings shall come under the same exclusion, as the majority of these are false. You should refer to your ICT specialists to check the validity of such messages but shall not forward these messages to anyone inside or outside the Trust under any circumstances.

- Emails of any kind shall not be sent to multiple external organisations without the appropriate approval of a senior staff member or teacher. This may be considered as ‘spamming’ which is an illegal activity in some countries.

- The individual logged in at a computer shall be considered to be the author of any messages sent from that computer. All ICT users shall log off or lock their computers when away from their desks; under no circumstances should a user send a message from somebody else’s account.

- Email addresses should not be disclosed unnecessarily. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.

- Email shall not be used to send large attached files, unless very urgent and authorised by the Systems Manager(s). Many email systems will not accept large files and, if returned may result in overloading the Learning Trust email system. Other media shall be used, such as encrypted USB's, when sending large amounts of data.

- Emails and attachments shall not be opened unless they are from a known source. Caution shall also be exercised even if attachments are received from a known source but are unexpected.

- The facility to automatically forward emails shall not be used to forward messages to personal email accounts. The Systems Manager(s) may be able to provide solutions for accessing the Learning Trust email system when working away from the office. Advice shall be sought from ICT if remote access is required.

- Emails may be archived by ICT Support to meet both the Learning Trusts requirements and any legal obligations.

3. Internet

The Talentum Learning Trust provides its students and employees with internet access to assist them in their learning and in the performance of their jobs. Whilst its use should primarily be official Learning Trust business, incidental and occasional personal use of the internet is permitted, on the understanding that:

- Personal use of the internet shall never impact the learning or business related internet access or upon the Trust's operational activities

- The Talentum Learning Trust reserves the right to curtail a student or employees' internet access to preserve its reputation and the integrity of its systems

- Messages shall not be posted on any internet message board or other similar Web based service that would bring The Talentum Learning Trust into disrepute, or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as those for email.

- Students or employees should not place on the internet, including social networking sites, any opinion or statement that might be construed as representing The Talentum Learning Trust.

- The Talentum Learning Trust shall report any illegal activity to the police. Students and employees will also be liable to The Talentum Learning Trust's own disciplinary process.

- Internet access shall not be used for personal financial gain, or to host a website on any The Talentum Learning Trust equipment without the express permission of the Executive Headteacher or a delegated officer.

- Students and employees shall not visit websites that display material of a pornographic nature, or contain material that could be considered offensive. System users should notify the ICT Support department(s) and/or Systems Manager(s) immediately should accidental access to such material occur. No disciplinary action shall be taken against students or employees who accidentally access sites containing dubious or unethical material providing they advise the System Manager in a timely manner. However in order to avoid disciplinary action, it is the students/employees responsibility to ensure that such unauthorised access does not happen on a frequent basis.

- Students and employees shall not download any files or software from the internet, or capture images that are displayed as there may well be any number of issues concerning copyright, malicious software and overall functioning of the computer and ICT systems.

- Students and employees logged into a computer shall be considered to be the person browsing the internet. Under no circumstances shall any student or employee browse the internet from an account belonging to another person.

- The Talentum Learning Trust will monitor and log all internet access by students and employees and reserve the right to disclose this information to any relevant authority.

- The Talentum Learning Trust establishment provided ICT equipment will be monitored at all times, both internally and remotely to ensure security and safety policies are being complied with.

4. Security Guidelines

Password Policy

Passwords should be:

- unique
- alphanumeric
- at least 8 characters in length
- regularly changed, recommend at least every 40 days

Passwords should NOT be:

- written down
- easy to guess
- shared with any other people including family and friends.

Monitoring Computer Use by Pupils

- Ensure pupil use of computers is visible, make sure there is a responsible person present and monitoring of use in place.
- Consider logging access to the network using software tools, for example NetSupport Tutor
- Review the layout of the room to ensure there is good 'visibility' of computer activities
- Publish the 'Rules of ICT Use' next to the computers, or consider displaying them on the screen when the computer is turned on
- Maintain an audit trail of user activity

Monitoring Computer Use by Staff (especially in sensitive areas)

- Use screensavers with passwords
- Think carefully about the siting / location of equipment
- Take care when disposing of paper output, floppy disks, computers etc that may contain sensitive or personal information
- Make staff aware that their use will be monitored and there should be no expectation of privacy.

System Backup

- Make sure the system is backed up regularly and checks are made that the backup has worked
- Try to implement an automated system backup
- Make sure the instructions for re-installing data or files from a backup are fully documented and readily available
- Where possible store the backup media in another building or a secure media safe
- You should periodically test a backup restore to make sure that the process works.
- Consider using different media as a secondary backup facility

Anti Virus Protection

- Always use an approved and recommended product
- Make sure there is a process to ensure it is regularly updated and ALL equipment is included, this is especially important for stand-alone PC's, laptops and PC's used at home
- Make sure there is a clear procedure for dealing with any actual or suspected infections
- Make sure the process for 'cleaning' infections is documented - this may involve requesting assistance from the 2nd Line Support Provider

For further advice on AV protection speak to the Information Security Team at Staffordshire County Council, or for help with procuring a product speak to the 2nd Line Support Provider.

Illegal or Inappropriate Use of the Network

- Make sure there are appropriate procedures in place for auditing access to the network and systems
- Regularly check the network for 'unauthorised' files
- If possible ensure auditing is performed both at the Management System level and also at the Operating System level (see section 11 below)
- Consider using appropriate software to assist with auditing - this can help monitor activities such as logons, file usage etc
- Consider using a firewall or proxy server to restrict external activity and access

Internet and Email Use

- Make sure an Internet and Email Use policy has been adopted for each 'category' of User and all Users have signed up to it
- Define and document any local agreements / policies on restricting web sites, access to newsgroups and chat-rooms etc
- Obtain parental permission where appropriate
- Ensure there is a clear process for reporting any access to inappropriate material
- Consider restricting specific functions such as the downloading of .exe files
- Publish safe guidelines
- Make sure Internet use is supervised
- Define and document any local policy on the use of email and email addresses, including the use of 'non-approved' email accounts
- Consider implementing limits on inbox sizes, size and types of attachments etc
- Be clear about what is considered 'appropriate' use of email and language
- Involve staff, parents and students in these decisions
- Use of websites such as ‘dropbox’ and ‘yousendit’ for file storage and transfer should be avoided where possible, it puts data at unnecessary risk and alternatives should be sought.

Documentation

Ensure adequate documentation is available for:

- The network infrastructure
- The network systems, hardware, software etc.
- Administration procedures
- Housekeeping procedures
- Problem resolution
- Ensure support disks, recovery disks, backups etc. are available

Training

- Ensure there is adequate training for System Managers and Users
- Introduce 'good practice' guidelines where appropriate e.g. using screen savers with passwords

Authentication / Operating System Level Security

- Consider using system policies to provide additional security
- Ensure there is a rigorous policy for approval / removal of Users
- Avoid the use of 'generic' accounts, where their use is unavoidable ensure they are set up only for the duration of the particular requirement.
- Limit the number of Administrator and Manager accounts
- Avoid the use of Groups with Administrator or Manager rights
- Only log on as Administrator or Manager when performing functions requiring this level of access, use an ordinary level User account where this is not required
- Set clear security levels on the network and ensure these are documented and followed
- Restrict access to applications and data areas where appropriate
- Consider using 'read only' access where possible

Network Review

- Monitor system downtime, ensure there are support arrangements in place to react to problems with critical equipment or infrastructure
- Monitor performance of the network - ensure there is a process in place to develop and upgrade the network infrastructure and equipment as necessary
- Monitor service disruption - ensure support arrangements are in place to resolve problems in a timely fashion
- Regularly review appropriate documents e.g. Computer Security policy, this could include reviewing official documents such as appropriate BECTA guidance
- Review procedures for dealing with all security breaches or compromises, whether deliberate or innocent

Monitoring Systems Usage

- It is important that you monitor the IT systems usage of all system users including internet and email use to make sure that the School's policy is being adhered to. However in order to comply with legislation including the European Convention of Human Rights and Fundamental Freedoms, The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 you must make all users aware that their usage will be monitored and why this monitoring is taking place.
- You should make all users aware that that the systems they are using are the property of the school and that there can be no expectation of privacy.
- You should make users aware that the school own the e-mail system which means that the school also own all copies of messages created, received or stored on the systems. The users should be made aware that no emails will be private, even if marked as "private" and/or "confidential" or with any similar wording.

Protective Marking

It is important to provide adequate protection to information, an additional tool which can assist in this is a protective marking scheme. All documents should be protectively marked, either using the government, or by an internal classification scheme.

For further information on protective marking we recommend that you speak to the County Council Information Security team. You should also read the guidance titled Good practice in Information Handling that starts on page 7 of the BECTA publication: *Good practice in information handling: Keeping data safe, secure and legal*.

A protective marking scheme is a way of assigning information to a security level which, in turn, relates to a range of pre-defined controls designed to ensure the information is handled properly.

From **6 April 2010** the Information Commissioner will have new powers to fine organisations up to a maximum of **£500,000** for data security breaches. A protective marking scheme is one of the activities you can undertake to ensure the security of the information that you hold.

Hardware and Software Inventory

- In order to comply with the School's Financial Regulations, you must maintain an inventory of all ICT equipment (however financed) which must be audited at least annually.
- The use of all private hardware for school purposes must be approved by the System Manager.
- A comprehensive inventory of all software and licence details should be maintained and regularly updated as software is acquired or disposed of. If software is used illegally because it is not licensed it could result in a fine or in extreme cases a jail sentence

For further information on software licensing go to http://www.fastiis.org/

Transferring Data

- Any data that is to be transferred outside of the school must be encrypted.
- Data held on USB storage devices, laptops or other removable media such as CDs must be encrypted to a minimum standard of 256 AES.
- Sensitive data that is being transferred by email must be encrypted.

Third Party Use

Rules for use of ICT Systems

This E-mail and Internet Use Good Practice statement will help protect third parties and The Talentum Learning Trust by clearly stating what is acceptable and what is not.

- The Talentum Learning Trust computer and Internet use must be appropriate for your education or professional use.
- Access must only be made via your authorised user account and password, which must NOT be given to any other person.
- Storage media must not be brought into any Talentum Learning Trust establishment unless prior permission has been given by the Systems Manager.
- The Talentum Learning Trust cannot be held responsible for the loss or corruption of *ANY* data you create or have created.
- Copyright and intellectual property rights must be respected
- Users must respect the work of others which might be stored in shared/common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored on the shared/common areas of the system must be transferred before the end of the Academic Year at which point they will be treated as temporary files and deleted.
- Users are responsible for the e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages, chain letters, hate inciting emails must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The Talentum Learning Trust ICT systems may not be used for private business purposes, unless explicit written permission has been given by the Executive Headteacher. Use for personal financial gain, gambling, political purposes or advertising is also forbidden.
- The security of any ICT system(s) must not be compromised, whoever they belong to.
- Irresponsible use may result in the loss of Internet access and Criminal Conviction.

The Talentum Learning Trust will exercise its right by electronic means to monitor the use of the Talentum Learning Trust's computer systems, including but not restricted to; remote monitoring of Talentum Learning Trust provided devices, the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Talentum Learning Trust computer system(s) is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Consent Form

For Third Party Use

The Talentum Learning Trust Responsible E-mail and Internet Use Please complete, sign and return to Systems Manager	
Name:	Address:
Start Date:	
Leaving Date:	
Agreement I have read and understand the Talentum Learning Trust 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	Date:

Rules for ICT Use – All Staff

In this policy, 'The Talentum Learning Trust', 'Learning Trust', or 'Trust' will be used to define all establishments within The Talentum Learning Trust, comprising of but not limited to Churnet View Middle School, Leek High School, and Westwood College.

	Notes
	You must not use, or try to use, Talentum Learning Trust's e-mail and internet facilities to create, distribute or display in any form any material that is or may be considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal). Anything that: • is pornographic or obscene, or includes any form of sexually explicit humour; • is intimidating, discriminatory (for example, racist, sexist or homophobic) • is defamatory, encourages violence or strong feelings; • is hateful; • is fraudulent; • shows or encourages violence or criminal acts; • may give the Talentum Learning Trust a bad name; or • is a deliberate harmful attack on any system Talentum Learning Trust, use, own or manage.
	Attempts to access unacceptable internet content will be treated the same whether the attempt was successful or not. Terms entered into search engines such as "Google" can be recorded and they will be considered as seriously as the content that would result from the search even if the content is blocked.
	You must not use the e-mail or internet facilities for time-wasting activities, such as chain letters, or for sending private e-mails to everyone on the global address list.
	When using Talentum Learning Trust e-mail facilities for private purposes to reduce the likelihood of The Talentum Learning Trust being targeted by spam, phishing or potential malicious activities you must not use your Trust email address when buying personal goods online
	You must not use or try to use Talentum Learning Trust ICT systems to access, without permission, any e-mail that is intended for another member of staff or an e-mail account of another member of staff.
	Ensure you know who is in charge of the ICT system you use, i.e. the System Manager(s).
	You must be aware that any infringement of the current legislation relating to the use of ICT systems, Personal or Corporate :- Data Protection Acts 1984 & 1998 or any subsequent revision General Data Protection Regulation (EU) 2018 or any subsequent revision General Data Protection Regulation (UK) 2018 or any subsequent revision Computer Misuse Act 1990 or any subsequent revision Copyright, Designs and Patents Act 1988 or any subsequent revision The Telecommunications Act 1984 or any subsequent revision Any additional legislation implemented by the UK Government **Breaches of this legislation may result in disciplinary, civil and/or criminal action**.

	You must follow any local rules determined by the Executive Headteacher or Headteacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be installed and/or used if approved by the Systems Manager(s) at the Talentum Learning Trust establishment you are located.
	You must ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. This includes if you are accessing systems from outside any Trust establishment including at home. Do not leave your computer logged on, i.e. where data can be directly accessed without password control, when not in attendance.
	You must not leave any computer unattended if you are accessing the Talentum Learning Trust systems on it unless the screen is locked i.e. it requires a password to gain access. This includes if you are accessing systems from outside any Trust establishment including at home.
	You must not exceed or attempt to exceed any access rights to systems or limitations on the use of data imposed on you by the System Manager(s). The ability to access information or systems is not the same as having authorisation to do so.
	The System Manager(s) will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a "made up" word, but not obvious or guessable, e.g. surname; date of birth, establishment name.
	<u>You must not share your user name and password with ANYONE (this includes but not restricted to family members and friends) unless specifically authorised to do so by the System Manager, e.g. in cases of shared access</u>
	Do not write your password down. You will be directly accountable for any network activity including internet and email use by your account.
	The System Manager(s) will advise you on what "back-ups" you need to make of the data and programs you use and the regularity and security of those backups.
	Users should make use of the OneDrive for Business storage, supplied as part of the Talentum Learning Trust, Office 365 tenancy. The use of 'mass storage' (USB, CDR, DVDR, BDR, HDD, etc.) devices are not permitted on the Trust ICT systems.
	You must ensure that newly received data storage devices (USB memory sticks, CD ROMs) and emails have been checked for viruses/malicious software. Any suspected or actual computer virus infection must be reported immediately to the System Manager.
	You must be vigilant for any suspicious ICT activity. You must immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Executive Headteacher.

	You must be aware that the data you create with Talentum Learning Trust equipment and systems remains the property of The Talentum Learning Trust. All data must be handled in accordance with any Protective Marking Scheme that may be in place.
	You must keep all business-related data on the Talentum Learning Trust network and not on the hard drive of your PC where practicably possible. Data that is stored on the Talentum Learning Trust network will be backed up on a regular basis
	You must lock sensitive data (hard copy and disks) away when not in use.
	You must ensure that sensitive data, both paper-based and electronic is disposed of properly – shred hardcopies and destroy disks.
	You must not store personal data (non Trust work) files including but not limited to personal MP3 files, personal photographs, personal music files and personal documents on the Talentum Learning Trust network(s), or Trust provided device (Laptop, Notebook, Tablet, iPad, Phone, Desktop), or storage media including the personal home folder/drives. The Talentum Learning Trust will not be held responsible for the deletion of any personal data
	You must make yourself aware of the contents of all other Information and ICT related policies such as the Talentum Learning Trust's e-Safety, Data Protection, and Social Networking policies.
	You must not copy files that are accessible centrally on any of the Talentum Learning Trust network(s) onto your personal home folder/drive on the network unless for amendment after which they must be deleted from the home drive. Wherever possible, work must be kept on shared network folder/drives and not on your home folder/drive.
	You must ensure that any data you take off site be it on a laptop, USB storage device or any other media is encrypted.
	You must not by manual or automatic methods, forward any emails sent to your Trust provided email address to another private/personal email account or service you own/lease/subscribe, unless permission has been received from the Trust Information Officer
	The Talentum Learning Trust will exercise its right by electronic means to monitor the use of the Trust's computer systems, including but not restricted to; remote monitoring of Trust provided devices, the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Monitoring is via a number of systems which may be global or establishment specific. These systems include, but are not limited to: Entrust ISP – Transparent Filtering and Usage Tracking Cisco Meraki Cloud based Mobile Device Management Future Digital – Future Cloud (Policy Central Enterprise) Impero Education Pro

	VNC TeamViewer Ubiquiti UniFi Microsoft Office 365 – Mobile Device Management pfSense Firewalls WatchGuard Firewalls
	Use of Social Media on Talentum Learning Trust or Privately Owned devices. Your Liability and the Law The law is clear that social media can be treated like any other media and account holders can be liable to criminal prosecution (for abuse, threats or revealing protected identities) and/or civil judgments for posting defamatory or offensive statements. **Crown Prosecution Service (CPS) guidance** The latest guidance in this area was issued by the Director of Public Prosecutions on 19 December 2012. It is worth noting that these are only interim guidelines and once the results of the March 2013 consultation on this area has been fully analysed, more detailed advice may be issued. **The interim guidelines** The interim guidelines draw a distinction between prosecutable communications that: constitute credible threats of violence to people or property specifically target an individual(s) for example, harassment, blackmail or stalking or amount to a breach of a court order, for example, Contempt of Court Act 1981 or s5 Sexual Offences (Amendment) Act 1992 which makes it an offence to publish material that leads to the identification of a victim of a sexual offence and communications that are: considered grossly offensive, indecent, obscene or false. The latter should be taken on a case-by-case basis and are unlikely to be in the public interest to proceed (criminally) unless they satisfy a high threshold. Indeed, the CPS guidance goes on to state that Article 10 of the Human Rights Act 1998 protects freedom of expression even where this speech is offensive, shocking or disturbing: Article 10 of the Human Rights Act 1998 protects freedom of expression even where this speech is offensive, shocking or disturbing. 'A communication sent has to be more than simply offensive to be contrary to the criminal law. Just because the content expressed in the communication is in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community, this is not in itself sufficient reason to engage the criminal law.' [34] 'Context is important and prosecutors should have regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place. Access is ubiquitous and instantaneous. Banter, jokes and offensive comments are commonplace and often spontaneous. Communications intended for a few may reach millions.' [35]

Talentum Learning Trust
ICT and Information Security Policy

Rules and Agreements for Staff

Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the Talentum Learning Trust's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users – Staff.

Your details

Name:

Job title:

Signature:

Date:

The Talentum Learning Trust

Comprising of:
Churnet View Middle School, Leek High School, and Westwood College

STUDENT

Rules for use of ICT Systems

The Talentum Learning Trust computer systems provide Internet access to students for learning. This E-mail and Internet Use Good Practice statement will help protect students and The Talentum Learning Trust by clearly stating what is acceptable and what is not.

- **The Talentum Learning Trust computer and Internet use must be appropriate for your education or professional use.**
- ***Access must only be made via your authorised user account and password, which must NOT be given to any other person.***
- **Users should make use of the OneDrive for Business storage, supplied as part of the Talentum Learning Trust, Office 365 tenancy. The use of 'mass storage' (USB, DVDR, BDR, HDD, etc.) devices are not permitted on the Trust ICT systems.**
- **The Talentum Learning Trust cannot be held responsible for the loss or corruption of *ANY* data you create.**
- **Copyright and intellectual property rights must be respected.**
- **Users must respect the work of others which might be stored in shared/common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored on the shared/common areas of the system must be transferred before the end of the Academic Year at which point they will be treated as temporary files and deleted.**
- **Users are responsible for the e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages, chain letters, hate inciting emails must not be sent.**
- **Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.**
- **The use of public chat rooms is not allowed.**
- **The Talentum Learning Trust ICT systems may not be used for private business purposes, unless explicit written permission has been given by the Executive** Headteacher**. Use for personal financial gain, gambling, political purposes or advertising is also forbidden.**
- **The security of any ICT system(s) must not be compromised, whoever they belong to.**
- **Irresponsible use may result in the loss of Internet access, or Permanent/Temporary Exclusion from the College, or Criminal Conviction.**
- **This Agreement also applies to any member of staff, or student using ICT systems whilst on Work Placement, Work Experience, or Secondment outside the Talentum Learning Trust.**

The Talentum Learning Trust will exercise its right by electronic means to monitor the use of the Talentum Learning Trust's computer systems, including but not restricted to; remote monitoring of Talentum Learning Trust provided devices, the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Talentum Learning Trust computer system(s) is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

1. You must not use, or try to use, the Talentum Learning Trust's e-mail and internet facilities to create, distribute or display in any form any material that is or may be considered to be illegal, offensive or unacceptable under our rules and policies. It is impossible to give a complete list of what is considered offensive or unacceptable, but the following are included (and in some cases may also be illegal).

   Anything that:

   - is pornographic or obscene, or includes any form of sexually explicit humour;
   - is intimidating, discriminatory (for example, racist, sexist or homophobic)
   - is defamatory, encourages violence or strong feelings;
   - is hateful;
   - is fraudulent;
   - shows or encourages violence or criminal acts;
   - may give the Talentum Learning Trust a bad name; or
   - is a deliberate harmful attack on any systems the Talentum Learning Trust use, own or manage.

2. Attempts to access unacceptable internet content will be treated the same whether the attempt was successful or not. Terms entered into search engines such as "Google" are recorded and they will be considered as seriously as the content that would result from the search even if the content is blocked.

3. You must not use the e-mail or internet facilities for time-wasting activities, such as chain letters, or for sending private e-mails to everyone on the global address list.

4. When using Talentum Learning Trust e-mail facilities for private purposes to reduce the likelihood of Talentum Learning Trust being targeted by spam, phishing or potential malicious activities. You must not use your Talentum Learning Trust email address when buying personal goods online.

5. You must not use or try to use Talentum Learning Trust systems to access, without permission, any e-mail that is intended for another member of staff or an e-mail account of another member of staff.

6. Ensure you know who is in charge of the ICT system you use, i.e. the System Manager.

7. You must be aware that any infringement of the current legislation relating to the use of ICT systems :-

   Data Protection Acts 1984 & 1998 or any subsequent revision
   General Data Protection Regulation (EU) 2018 or any subsequent revision
   General Data Protection Regulation (UK) 2018 or any subsequent revision
   Computer Misuse Act 1990 or any subsequent revision
   Copyright, Designs and Patents Act 1988 or any subsequent revision
   The Telecommunications Act 1984 or any subsequent revision
   Any additional legislation implemented by the UK Government

   Breaches of this legislation may result in disciplinary, civil and/or criminal action.

8. You must follow any local rules determined by the Executive Headteacher in relation to the use of private equipment and software.
   All software must be used strictly in accordance the terms of its licence and may only be used if approved by the Systems Manager.

9. You must ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. This includes if you are accessing systems from outside of any Talentum Learning Trust establishment including at home.

Do not leave your computer logged on, i.e. where data can be directly accessed without password control, when not in attendance.

10. You must not leave any computer unattended if you are accessing The Talentum Learning Trust systems on it unless the screen is locked i.e. it requires a password to gain access. This includes if you are accessing systems from outside any Talentum Learning Trust establishment including at home.

11. You must not exceed any access rights to systems or limitations on the use of data imposed on you by the System Manager. The ability to access information or systems is not the same as having authorisation to do so.

12. The System Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use.
    You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a "made up" word, but not obvious or guessable, e.g. surname; date of birth, establishment name.

13. **You must not share your user name and password with ANYONE (this includes but not restricted to family members and friends) unless specifically authorised to do so by the System Manager, e.g. in cases of shared access**

14. Do not write your password down. You will be directly accountable for any network activity including internet and email use by your account.

15. The System Manager will advise you on what "backups" you need to make of the data and programs you use and the regularity and security of those backups.

16. You must ensure that newly received data storage devices (USB memory sticks, CD ROMs, etc.) and emails attachments have been checked for computer viruses.
    Any suspected or actual computer virus infection must be reported immediately to the System Manager.

17. You must be vigilant for any suspicious ICT activity. You must immediately report any suspected or actual breach of ICT security to the System Manager or, in exceptional cases, the Executive Headteacher.

18. You must be aware that the data you create with Talentum Learning Trust equipment and systems remains the property of The Talentum Learning Trust. All data must be handled in accordance with any Protective Marking Scheme that may be in place.

19. You must keep all business-related data on the Talentum Learning Trust network(s) and not on the hard drive of your PC where practicably possible. Data that is stored on The Talentum Learning Trust network(s) will be backed up on a regular basis.

20. You must lock sensitive data (hard copy and disks) away when not in use to comply with the Data Protection Act and General Data Protection Regulations (UK and EU), or any subsequent revisions or Acts.

21. You must ensure that sensitive data, both paper-based and electronic is disposed of properly - shred hardcopies and destroy disks to comply with the Data Protection Act and General Data Protection Regulations (UK and EU), or any subsequent revisions or Acts.

22. You must not store personal data (non-Talentum Learning Trust work) files including but not limited to personal MP3 files, personal photographs, personal music files and personal documents on the Talentum Learning Trust network(s), or Talentum Learning Trust provided device (Laptop, Notebook, Tablet, iPad, Phone, Desktop), or storage media including the personal home folder/drives. The Talentum Learning Trust

will not be held responsible for the loss or deletion of any personal data.

23. You must make yourself aware of the contents of all other ICT related policies such as the Talentum Learning Trust's e-Safety, Data Protection, and Social Networking policies.

24. You must not copy files that are accessible centrally on the Talentum Learning Trust network(s) onto your personal home folder/drive on the network unless for amendment after which they must be deleted from the home drive. Wherever possible, work must be kept on shared network folder/drives and not on your home folder/drive.

25. **You must ensure that any data you take off site be it on a notebook, Laptop, Tablet, iPad, USB storage device or any other media is encrypted.**

26. The Talentum Learning Trust will exercise its right by electronic means to monitor the use of the Trust's computer systems, including but not restricted to; remote monitoring of Trust provided devices, the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

    Monitoring is via a number of systems which may be global or establishment specific. These systems include, but are not limited to:
    Entrust ISP – Transparent Filtering and Usage Tracking
    Cisco Meraki Cloud based Mobile Device Management
    Future Digital – Future Cloud (Policy Central Enterprise)
    Impero Education Pro
    VNC
    TeanViewer
    Ubiquiti UniFi
    Microsoft Office 365 – Mobile Device Management
    pfSense Firewalls
    WatchGuard Firewalls

Consent Form For Students

The Talentum Learning Trust
Comprising of:
Churnet View Middle School, Leek High School, and Westwood College

Responsible E-mail and Internet Use

Please complete, sign and return to your Tutor

Pupil:	***Form:***

Pupil's Agreement

I have read and understand the Talentum Learning Trust 'E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed:	***Date:***

Parent / Carer's Consent for Internet Access

I have read and understood the Talentum Learning Trust 'E-mail and Internet Use Good Practice - Rules for ICT Users' document and give permission for my son / daughter to access the Internet. I understand that the Talentum Learning Trust will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the Talentum Learning Trust cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the Talentum Learning Trust is not liable for any loss or damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Parent / Carer's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on any of the Talentum Learning Trusts web or social media sites. I also agree that photographs that include my son/daughter may be published subject to the Talentum Learning Trust rules that photographs will not clearly identify individuals and that full names will not be used.

Signed:	***Date:***

Staffordshire County Council
Recommended Backup Strategy for Schools

All data should be backed up at least 3 times each week – for example, Monday, Wednesday & Friday. This will ensure that at least three copies of the data will always be available. (In the case of a large school, processing large amounts of data daily, a backup every day should be taken.)

At least one of the backups should ideally be kept in a separate secure building on the school premises to the schools' servers (in case of fire or theft). If this is not possible a fire-proof media safe somewhere on site would be an ideal alternative.

All backups should be checked to ensure that they have been successful. (E.g. If a backup has been made to a tape, the contents of the tape should be checked to see that a file, or files exist, and that their date of creation is consistent with the date of the backup.)

A 'Long Term Backup' should be taken at the beginning of each term. This should be kept and not overwritten until the beginning of the next term. This will help protect against data corruption that may go unnoticed for several weeks, during which 'older' backups will have been overwritten by 'newer' ones.

Differing media are employed in schools for backing up purposes. E.g. Magnetic tapes, hard disks, USB drives. If you suspect your Headteacher backup medium is not working correctly (tape drives can be unreliable), use an alternative, until the problem is corrected.

If possible, use more than one medium for backup. For network users, the option to record onto workstation hard disks is always available. Do this as well as taking an alternative backup.

If you are unsure about your backups - please telephone the Staffordshire SLT Service Desk and check whether or not your current processes are adequate and reliable.

You should periodically do a restore from a backup to ensure that the process works and all the data has been successfully backed up.

9. Churnet View Middle School - Backup Strategy

10. Leek High School - Backup Strategy

11. Westwood College - Backup Strategy

- The College uses Veeam Essentials to perform routine backups of its server estate.
- Full backups are taken every Friday.

  Weekly backups are stored [redacted].

  They are kept for 60 Days, and then overwritten.

  Monthly Backups are [redacted].

  They are Kept for 12 months, and then overwritten.
- Incremental backups are taken Monday thru to Thursday, [redacted], and overwritten on a 4 weekly basis.
- Weekly User and MIS data backups are removed from site using RDX cartridges.

  6 cartridges are held [redacted].
- Full Backups are encrypted to AES 256bit encryption.
- Restoration tests of backups are carried out regularly, where practicably possible at the end of every term.
- User Data is archived to RDX cartridge each August, and stored [redacted].
- The Backup software reports via Email to the ICT Support team to outcome of each and every backup/restore process.

12. Guidance for Repair and Disposal

Staffordshire County Council Guidance for:
Repair and Disposal of ICT Equipment and Disposal of Waste

Repair
If a piece of ICT equipment is in need of repair, consideration needs to be given to the sensitivity of any data that may be on the device. If the data on the device is particularly sensitive, then it will need to be removed and placed securely in network storage before the device is handed over for repair.

Ideally a written agreement should be in place between the school and any repairer, stating agreed levels of confidentiality and reinforcing the sensitivity of schools data.

If possible the schools should ensure that any third parties utilised for repairing equipment are registered under the Data Protection Act as personnel authorised to see data, as such they would be bound by the same rules as school staff in relation to not divulging data or making any unauthorised use of it.

Disposal of ICT Equipment
Prior to the transfer or disposal of any ICT equipment the System Manager or an authorised individual must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

The Data Protection Act requires that any personal data held on such a machine be destroyed.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

Disposal of Waste
Disposal of waste ICT media such as print-outs, CDs, Hard Drives and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper and CDs will be shredded if any confidential information could be derived from them.

The Data Protection Act and General Data Protection Regulation (EU and UK) requires that adequate mechanisms be used when disposing of personal data.

13. Churnet View Middle School - Disposal Procedure

14. Leek High School - Disposal Procedure

15. Westwood College - Disposal Procedure

Westwood College utilises EnviroElectronics Ltd to dispose of unwanted electrical and electronic items.

Company Number: 07841186

Contact Details:
Unit 69 Wright Business Park
Balby Carr Bank
Doncaster
South Yorkshire
DN4 8DE

Office Tel: 01302 376494

Waste Carrier License: CB/ZE5890VK
Waste Permit Number: NCC/059618/2012
Hazardous Waste Registration: OFJ094

All devices are disposed of to relevant UK Standards.

All data is destroyed using the relevant standard(s) listed below:
PCI DSS – Payment Card Industry Data Security Standard
HIPAA – Health Information Portability and Accountability Act
PIPEDA – Personal Information Protection and Electronic Documents Act
Data Protection Act 1998
General Data Protection Regulation (EU and UK) 2018

16. Hardware Inventory

Establishment: **Churnet View Middle School**	*DfEE No:* **4160**
Establishment Contact: [redacted]	*Phone No:* **01538 384939**
Email Address: [redacted]	*Date of Last Audit:*
NOTES:	

Establishment: **Leek High School**	*DfEE No:* **4085**
Establishment Contact: [redacted]	*Phone No:* **01538 225050**
Email Address: [redacted]	*Date of Last Audit:*
NOTES:	

Establishment: **Westwood College**	*DfEE No:* **4086**
Establishment Contact: **Duncan Smith**	*Phone No:* **01538 370930**
Email Address: **westwoodictsupport@leekfederation.org.uk**	*Date of Last Audit:* **AUG-2016**
NOTES: **ICT Hardware inventory located on the AssetGuard Pro system, separate to this document.**	

Procedure for Security Protocols following Suspension/Dismissal/Retirement/Resignation of members of the Senior Leadership Team (SLT) or ICT Support Team.

Definitions for this Procedure

A member of the Senior Leadership Team is defined as;

'Any member of The Talentum Learning Trust, or Individual Establishment staff who has raised access rights over ANY of The Talentum Learning Trust or any individual establishment within The Talentum Learning Trusts' ICT System(s)/Network(s) and/or Security/Intruder System(s)'.

A member of the ICT Support Team is defined as;

'***Any member of The Talentum Learning Trust, and/or Individual Establishment staff who has raised access rights over ANY of The Talentum Learning Trust or any individual establishment within The Talentum Learning Trusts' ICT System(s)/Network(s), and/or Security/Intruder System(s)'***

ICT System(s)/Network(s) is defined as;

'Any ICT system/facility/service, either on premise or cloud based, owned, leased, or aquired by The Talentum Learning Trust or any individual establishment within The Talentum Learning Trust.'

Security/Intruder Systems are defined as;

'Any Security/Intruder Detection system/facility/service, either on premise or cloud based, owned, leased, or aquired by The Talentum Learning Trust or any individual establishment within The Talentum Learning Trust.'

Headteacher is defined as;

Executive Headteacher***, Headteacher, Associate Headteacher or any other member of The Talentum Learning Trust or any individual establishment within The Talentum Learning Trusts', Senior Management / Leadership Team.***

A list of these staff members is available in **APPENDIX 1** of the Information and ICT Security Policy.
Due to the sensitive nature of this part of this policy the document can be seen on request.

NOTE:

IF THE SITUATION IS DEEMED TO BE OF A VERY SERIOUS NATURE, THE ESTABLISHMENTS' INTERNET ROUTER(S) SHOULD BE POWERED OFF, BEFORE THE STAFF MEMBER LEAVES THE PREMESIS.

This will cause issues with Staff in the Finance and HR Offices – They should be notified ASAP before the Router(s) is/are turned OFF to minimise any possible data corruption within the Financial, Payroll, and HR systems.

IF THE HEADTEACHER REQUIRES IT, THEN ALL THE ESTABLISHMENTS SERVERS SHOULD BE SHUT DOWN, AND POWERED OFF UNTIL ANY POSSIBLE BREECH OF SECURITY IS MINIMISED.

THIS WILL STOP ANY EXTERNAL ACCESS TO THE ESTABLISHMENTS ICT SYSTEMS

The following Procedures can then be followed, with reduced risk to the Talentum Learning Trust's or any individual establishment within the Talentum Learning Trusts' ICT Systems or Network(s).

18. Churnet View Middle School – Procedure

19. Leek High School – Procedure

20. Westwood College - Procedure

Procedure for Dismissal or Resignation/Retirement of a member of SLT or ICT Support Staff

*The following needs to take place **BEFORE** the member of staff leaves the College Premises, **IF** the parts below are relevant to their role;*

- Staff members' network accounts need to be ***disabled***, and ***expired*** on College and/or Talentum Learning Trust ICT Systems and/or Network(s). – The Systems Manager at each establishment may need notifying, if the staff member has access at more than one establishment.

[redacted]

Procedure for Suspension of a member of SLT or ICT Support Staff

*The following needs to take place **BEFORE** the member of staff leaves the College Premises, IF relevant to their role;*

- Staff members' network accounts need to be ***disabled***, and ***expired*** on College and/or Talentum Learning Trust ICT Systems and Networks.

[redacted]

- If known to Staff Member – **Intruder Alarm Codes and/or Access Fob** needs to be disabled/returned.

The following needs to be completed as soon as possible AFTER the member of staff has been escorted from the College premises;

- Locks need to be changed on the following doors, if the Headteacher or Systems Manager decide it necessary;
    - Main Entrance Doors
    - Server Room – Outer and Inner Doors
    - Boiler House – Old Hall

21. Document Information per Establishment

Nominated System Managers:	Churnet View:	[redacted]
	Leek High School:	[redacted]
	Westwood College:	**Duncan V. Smith**

Churnet View Middle School

Document Name	SCC Model document or Schools own?	Location of Document	Produced / Reviewed By	Last Review Date	Date next Review is due
Information Security Policy	Modified				MAY-2019
Part 9 - Backup Strategy	Modified				MAY-2019
Part 13 - Repair and Disposal	Modified				MAY-2019
Part 18 – Security Protocols	Modified				MAY-2019
APPENDIX 1 - Staff List for Section 18	Modified				MAY-2019

Leek High School

Document Name	SCC Model document or Schools own?	Location of Document	Produced / Reviewed By	Last Review Date	Date next Review is due
Information Security Policy	Modified				MAY-2019
Part 10 - Backup Strategy	Modified				MAY-2019
Part 14 - Repair and Disposal	Modified				MAY-2019
Part 19 – Security Protocols	Modified				MAY-2019
APPENDIX 1 - Staff List for Section 19	Modified				MAY-2019

Westwood College

Document Name	SCC Model document or Schools own?	Location of Document	Produced / Reviewed By	Last Review Date	Date next Review is due
Information Security Policy	Modified	Staff Shared Resources	SMD	06-JUN-2018	MAY-2019
Part 11 - Backup Strategy	Modified	Staff Shared Resources	SMD	06-JUN-2018	MAY-2019
Part 15 - Repair and Disposal	Modified	Staff Shared Resources	SMD	06-JUN-2018	MAY-2019
Part 20 – Security Protocols	Modified	Staff Shared Resources	SMD	06-JUN-2018	MAY-2019
APPENDIX 1 - Staff List for Section 20	Modified	Staff Shared Resources	SMD	06-JUN-2018	MAY-2019

22. NOTES

Westwood College have implemented a system to make users electronically sign and agree to the Information and ICT Security Policy every time they logon to a College provided computer.

END OF DOCUMENT