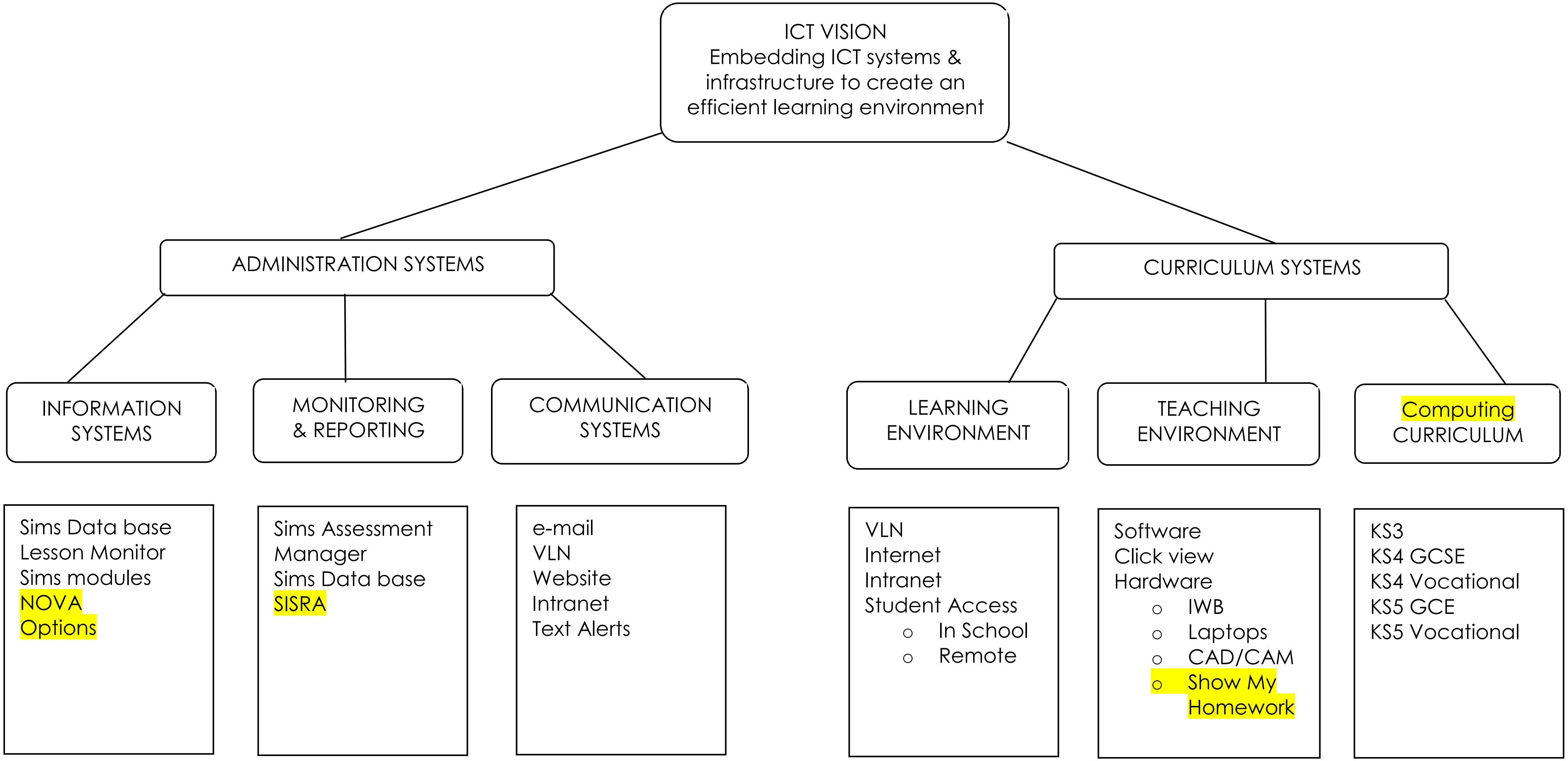
The Deanery

Church of England High School and Sixth Form College

ICT
POLICY

MAY 2015

ICT Strands in the Deanery High School



ICT VISION
Embedding ICT systems & infrastructure to create an efficient learning environment

ADMINISTRATION SYSTEMS

INFORMATION SYSTEMS

Sims Data base
Lesson Monitor
Sims modules
NOVA
Options

MONITORING & REPORTING

Sims Assessment Manager
Sims Data base
SISRA

COMMUNICATION SYSTEMS

e-mail
VLN
Website
Intranet
Text Alerts

CURRICULUM SYSTEMS

LEARNING ENVIRONMENT

VLN
Internet
Intranet
Student Access
- In School
- Remote

TEACHING ENVIRONMENT

Software
Click view
Hardware
- IWB
- Laptops
- CAD/CAM
- Show My Homework

Computing CURRICULUM

KS3
KS4 GCSE
KS4 Vocational
KS5 GCE
KS5 Vocational

Rationale

The purpose of this policy is to set out a clear vision for the provision of ICT facilities and Computing education throughout the Deanery High School. It is intended that this policy will be a working document that can be used to help drive present and future developments and to influence budget decisions.

The document seeks to describe both current provision and vision for the future in each of several key areas.

Vision

We aim to develop and embed ICT systems & infrastructure that will create essential administrative tools and an efficient learning environment. The diagram at the start of this document identifies the various strands of ICT that are currently in place in each of the key areas. In a rapidly changing field such as ICT, it is of course impossible to say what technologies will be available in the future; it is however possible to state in general terms how we intend to use ICT for the benefit of our school.

CURRICULUM SYSTEMS

Learning Environment

ICT in all its different facets can open up a whole world of learning for young people. We aim to provide quality ICT facilities, to which all children can have easy and equal access. Through our teaching in all curriculum areas we aim to develop children's ICT skills so that they are able to make best use of the ICT facilities as a modern learning tool. We aim to prepare children for a world where mastery of ICT and adaptability to new technologies is critical to their future wellbeing and prosperity.

To achieve this we will ensure that:

- There is an efficient and reliable curriculum based network.
- There is modern up to date software.
- There is internet access with effective monitoring and filtering software.
- That all students are regularly instructed in safe e-learning (CEOP).
- Development of resource sharing systems (VLN or intranet).
- Access to new technologies as and when appropriate.
- All students have maximum possible access to all of the above including:
    - Access in school.
    - Remote access from home.

Relevant Processes

- Student Acceptable Use Statement: To be electronically approved by all student users (see Appendix 1)
- Subject Improvement Plans: All subject leaders are responsible for the writing and submission of improvement plans in which they will give due consideration to the development of ICT within their faculty/subject.
- Maintaining and reporting issues arising from monitoring and filtering software.

Teaching Environment

ICT as a set of teaching tools has opened up a wide new range of resources and made many new teaching styles a possibility. We aim to ensure that the best possible resources both hardware and software are available to staff. We also aim to ensure that staff have the best possible access to these resources and are fully trained to use them to maximum potential.

To achieve this we will ensure that:

- There is an efficient and reliable curriculum based network.
- There is modern up-to-date software.
- There is internet access with effective monitoring and filtering software.
- Development of resource sharing systems (VLN or intranet).
- Maximum possible access to hardware and software e.g. Interactive White Boards, Voting systems, Click View, and other subject specific systems.
- Access to new technologies with suitable training as and when appropriate.
- All teachers have maximum possible access to all of the above including:
    - Access in school.

- Remote access from home.

Relevant Processes

- Staff Acceptable Use Statement: To be approved electronically by all staff users (see Appendix 2).
- Subject Action Plans - all subject leaders are responsible for the writing and submission of Action plans in which they will give due consideration to the development of ICT within their faculty/subject.
- Training needs identified through the performance management process, and inset delivered as appropriate (Assistant Head: Staff Development).
- Induction for all new staff to the school's ICT systems and technologies (see Appendix 5) - Assistant Head: Staff Development.

Computing Curriculum

The curriculum has now all but abandoned the teaching of ICT in favour of Computer Science. Our courses will all be compliant with National Curriculum requirements and will seek to maintain both Computing and ICT courses at examination level where demand exists.

To achieve this we will offer a range of courses which may include:

- KS3 courses in line with National Curriculum requirements.
- KS4 GCSE in Computer Science
- KS4 GCSE in ICT
- KS4 GCSE in iMedia.
- KS5 GCE in iMedia, ICT, Computer Science
- KS5 Level 3 BTEC ICT Systems(formerly CISCO).

Relevant Processes

- Subject Action Plans: All subject leaders are responsible for the writing and submission of improvement plans in which they will give due consideration to the development of ICT within their faculty / subject.

ADMINISTRATION SYSTEMS

Information Systems

Maintaining complete and up to date information in school databases is essential to the smooth running of the school. This in turn ensures the core business of the school, i.e. learning is as efficient as possible. We aim to develop the use of ICT to ensure all school information is as accurate as possible and accessible as necessary. We will take all necessary steps to ensure the security of all confidential information in line with the Data Protection Act.

To achieve this we will ensure that:

- The Sims database is regularly updated with pupil and staff details.
- The Sims software is kept up to date through the installation of software updates.
- That appropriate Sims modules are used to ease administrative tasks wherever possible. At the moment this includes:
  - Personnel modules.
  - Nova T6 timetable modules.
  - Course manager.
  - Lesson monitor.
  - Financial modules.
  - Examination modules.
  - Assessment Manager.
- That census returns are accurate and competed on time.
- That data backups are made on a daily basis.
- That a register of users and access levels for sims is maintained and access only granted on completion of a signed form by a member of the SLT.

Relevant Processes

- Updating pupil database.

- Updating staff database.
- Register of staff access and access level.
- Granting of access rights to Sims.
- Completion of census returns.
- Sims updates and data back up.

Monitoring & Reporting Systems

Monitoring, analysis and reporting of pupil progress is essential in helping pupils to achieve. We consider that the monitoring of attendance, pupil incidents, and behavioural issues are keys to delivering good quality pastoral care. We aim to make optimum use of ICT to assist staff in this area.

To achieve this we will ensure that:

- The sims database is regularly updated with pupil and staff details.
- The sims software is kept up to date through the installation of software updates.
- That appropriate sims modules are used to ease administrative tasks wherever possible.
- That there are ICT facilities to help record and analyse pupil progress. That staff training and induction is carried out to ensure staff are adequately trained.
- That on line access for parents to pupil data is established in line with statutory requirements (not yet in place).

Relevant Processes

- Updating pupil database.
- Sims updates and data back up.
- Maintaining monitoring and reporting details in sims assessment manager and SISRA.
- Pupil data input to pupiltracker.com at times specified on school calendar.

Communication Systems

We recognise that good communications between all school stakeholders is essential to the smooth running of the school. We aim to ensure that there are adequate ICT facilities to ensure that information can be shared quickly and efficiently.

To achieve this we will ensure that:

- Staff have ready access to e-mail both within school and remotely.
- We develop an effective web site and establish systems to ensure that information is regularly updated.
- We develop the use of our VLN as a vehicle for sharing information and teaching resources.
- We develop processes for communication with parents including text alert systems, and online access to pupil data in line with statutory requirements.
- We develop the use of TV display screens around school.

Relevant Processes

- Updating and expanding the school website.
- Development of intranet/VLN.

Roles & Responsibilities

Task	**Person Responsible**
Completion of student acceptable use statements	Computing Faculty
Subject Action Plans	HoFs & HoDs
Maintaining monitoring & filtering software	Network Manager
Completion of staff acceptable use statements	Deputy Head: Curriculum
Staff training needs for ICT	Assistant Head: Staff Development
New staff induction	Assistant Head: Staff Development
Computing Curriculum	Head of Computing Faculty

Updating SIMS pupil information	Pastoral Managers
Updating SIMS staff information	Office Manager
Maintaining a register of SIMS users and access levels	Sims manager
Granting SIMS access rights	Deputy Head: Curriculum
Completion of school census returns	Pastoral Manager: Sims
Installing SIMS updates, data back up and security	Sims manager
Maintain SIMS Assessment Manager & SISRA for monitoring and reporting	Data manager
Pupil Tracker data input for pupil progress	All Staff
Web site update	ICT Support
Text Alert systems	Ext Relations
TV information screens	Ext Relations
VLN Development	VLN Staff Leader

Procedures for dealing with inappropriate use.

Although communication via the Internet will be filtered, access to unsuitable material may still be possible. Where this happens accidentally the following action to reduce the risk of repetition must be implemented.

1 The staff involved must record details of the circumstances and inform the Senior Leader with oversight of ICT.

2 The Senior Leader must:

- review local filtering.
- request appropriate adjustment to the filter policy.
- notify the education department if appropriate.

Where deliberate and malicious inappropriate use of the intranet or Internet is suspected the matter must be reported immediately to the Senior Leader where appropriate. S/he should take the following action:

- review procedures to prevent further repetition and to ensure the safety of pupils.
- make security copies of any files or logs related to the incident.
- initiate a formal investigation and consider referral to the formal disciplinary procedures.

The Senior Leader must maintain a record of all instances of significant misuse of the Internet.

This policy was approved by the Curriculum Committee on 13th May 2015.

Next review date: May 2017

Appendix 1

Acceptable Use Guidelines: Pupils

ICT Acceptable Use

- I will not access computer files belonging to others.
- I will access the school network using my own password only.
- I will access only those computer discs and DVDs for which the teacher has given me permission.
- I will ensure that any e-mails I send are polite, sensible and responsible
- I will only send e-mails to people I know or who are approved by my teacher. I will not forward chain letters nor send defamatory emails.
- I will use my official school e-mail account only to send or receive e-mails.
- I will tell a teacher if I see web pages or e-mails which are offensive or unpleasant.
- I understand that the school will use monitoring software to check my computer files, e-mails and the Internet sites which I visit to ensure that I use the computer and the Internet properly. Inappropriate use will result in 'screen shots' of my computer being automatically taken and sent to my pastoral team.
- I will only access the Internet for educational purposes and not for advertising, gambling or political purposes.
- I will only download material from the Internet which could not be seen as offensive in any way.
- I will only copy and use material as allowed by copyright legislation i.e. where prior permission for copying has been given. I will ask my teacher if I am not sure of the legal position.
- When using the Internet and sending e-mails I will protect myself and others by not giving:
  my name
  my home address
  my home telephone number
  my photograph
  any other personal information
  any information about others.
- I will not arrange to meet any on-line contact. I will tell my teacher about any invitations to meet on-line contacts.
- I will not attempt to install software, bypass security systems, carry out any illegal actions or interfere in any way with the operation of the school network.
- I will not connect any pen drive or other data storage device to the school network that contains any material other than my school / college work. (In particular I will not attempt to run games from a pen drive)

Pupil's Name: ____

Pupil's Signature: ____ Date: ______________

Parent's Signature: ____

Appendix 2

Letter to Parents

Dear Parent

The School network and Internet Use

The Internet is an increasing feature of everyday life. Pupils will have access to our computer network and the internet in school to ensure that they are given the opportunity to develop their Information and Communications Technology (ICT) skills.

Along with its benefits the Internet also brings risks. Mixed with the vast amount of good, useful information on the Internet there is some which is inappropriate and potentially harmful to children. To protect pupils, our Internet service provider performs rigorous filtering of the World Wide Web, newsgroups and electronic mail for inappropriate and offensive material. Further monitoring and filtering takes place within school to ensure maximum possible protection. Nevertheless you should be aware that the potential to access inappropriate material does exist and that no filtering technology can completely guarantee that a pupil will never come across distasteful material in some form or other.

Before being allowed to use the school network and access the Internet, all pupils will be required to agree to and sign the schools ICT Acceptable Use Statement (copy enclosed). The school needs your support in expecting pupils to use their access to the school network and the Internet in an ethical and responsible manner at all times, You are therefore asked to counter-sign the Acceptable Use Statement completed by your son/daughter to confirm your approval and their acceptance of the school rules on this matter.

From time to time the school may publish photos of pupils and pupils work on the school website and in the local press **but** personal details and individual photos will not be used without permission. Should parents not wish this publication they should write to the school.

Yours sincerely

Mrs J Rowlands
Headteacher

Acceptable Use Guidelines: Staff / Governors

ICT Acceptable Use

- Before you can use the ICT resources at the Deanery High School you must agree to the following acceptable use rules.
- This applies to all adults who have been granted a username and password for the school network and ICT facilities.
- Once you have signed and dated the policy it will be stored centrally until you no longer have a username for the systems.

Computer / User usage policy

- Users must not install, or attempt to install, programs of any type on a machine, or store programs on the computers, without permission from the Network Manager.
- Users must not damage, disable or otherwise harm the operation of computers and peripherals, or intentionally waste limited resources.
- Users will not use the school's ICT resources for commercial purposes, e.g. running a business.
- Users will not disclose their password(s) to anyone else.
- Users will be required to change their passwords periodically.
- Users must not use passwords intended for the use of others.
- Users making use of the network must do so in a way that does not harm, harass, offend or insult others.
- Users are expected to respect all security systems and must not attempt to bypass any of the security in place on the computer systems. All network activity including key strokes, and internet use is monitored by security software. Should this software spot a 'violation', a screen shot will be automatically taken and sent to the Deputy Head (Curriculum).
- Users must not attempt to access, copy, remove or otherwise alter other peoples work, or attempt to alter the settings of computers.
- Users must report all suspicious activity to the Network Manager or MIS Technical Manager immediately.
- Users must report all damage, faults and security breaches to the Network Manager.
- Users must not leave a school computer logged on and unattended in an area where children could access it. This is particularly important if you are logged onto sims.
  (Should you wish to leave the computer for a short while you can lock it with a CTRL + ALT + DEL action. It is then quickly unlocked on your return by entering your password).

Internet usage policy

- Users must not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Users are expected to respect the work and ownership rights of people outside the school as well as Users and staff. This includes abiding by copyright and plagiarism laws.
- Users will not give personal information such as addresses or telephone numbers of themselves, staff or others to those they contact via the internet.
- The activities of all Users will be logged whilst using the Internet.
- Users may use the E-Mail system to transfer their own files between school and home.
- Users must NOT send any messages that are offensive or in bad taste
- ALL messages MUST be sent in your own name. You must NOT impersonate other users
- If you receive an Email you think may be forged you MUST forward a copy to the Network Manager.

You are advised that the school network is a corporate system and as such any information, data files and e-mails could be subject freedom of information, or data protection requests.

- When You Tube is made available to staff it must only be used as a lesson / assembly resource. Staff should be aware of possible dangers of inappropriate material being inadvertently displayed. You Tube videos should only be shown to children when embedded into a PowerPoint or other office application. Staff should not search the You Tube site in front of children. (Embedding a clip is very easy. There are You Tube videos to show you how to do this).

Data Protection

- All electronic communication and data relating to Deanery High School, staff and students, must be considered confidential.
- Confidential material as defined above must not be shared or discussed outside the Deanery High School by any means but with particular respect to social networking media.
- Staff must ensure that children's personal data cannot be seen by other children. This applies particularly to electronic registration when interactive white boards should be 'blanked' or 'frozen' so children cannot see the attendance marks of other children.
- Photographs of children from sims should not be left around school.

Staff who need to be able to access sims from home will be allowed to do so with the permission of the appropriate line manager. In doing so they accept responsibility for the security of the data. Staff must not disclose their sims password to anyone. They must ensure that sims cannot be accessed by anyone in their home who is not authorized to do so.

Under **no** circumstances, should information from sims be passed to third parties, or used for any purpose other than normal school business.

Confidential data should not be stored on portable or home devices. Any work on confidential data should be done via a remote log on to the school network. This ensures that confidential data never leaves the school network.

Home computers and portable storage devices, e.g. pen drives. Should only be used for non-confidential data.

I confirm that I have read and agree to abide by the staff acceptable use policy.

Signed: ___________________________

Print: _____________________________

Date: _______ / ________ / ___________

Action to be taken in the event of suspected abuse

School Laptops / IT Facilities

Further to the letter issued by Children and Young People's Services on **27th** June, 2006 concerning the above, schools should as far as possible, carry out the attached procedures when it is suspected that computer equipment may hold evidence of misuse that may be required as part of an internal or external investigation.

The advice given is based on A Good Practice Guide for Computer based Electronic Evidence issued by the Association of Chief Police Officers (ACPO). It is recognised that some of the procedures outlined by ACPO may not be possible in the school environment but it is important that the guidance should be followed as closely as possible in order to preserve evidence that may, ultimately, be required in a criminal prosecution.

Laptop Computers

If an allegation of inappropriate use of computing facilities is made against a user:

1. Remove the computer from the user's possession including mouse and all leads and cables.

2. Don't, under any circumstances, switch the computer on.

3. Some laptop computers are powered on by opening the lid. Therefore, as a precaution, remove the battery.

4. Remove any other storage media from the user, for example, CDs, floppy disks, pen drives, digital cameras, external hard drives etc.

5. Make an inventory of what's been taken from the user, recording unique identifiers, for example, serial numbers. Get the inventory independently verified and signed.

6. Ensure that all items have signed and completed labels attached in order to preserve continuity of evidence. The labels should describe the type, model, serial number etc of the equipment.

7. Ask the user whether there are any logon user ids and passwords required and, if so, record them accurately.

8. Make detailed notes of all actions taken in relation to the computer equipment on the attached pro-forma.

9. The computer and related equipment must be stored in a secure location until collected.

10. The allegation and actions taken should immediately be reported to the IT Manager within Children and Young People's Services (01942 486063) and they will make arrangements for a forensic examination of the computer.

11. Further advice should be obtained from Corporate Personnel Services.

If indecent or inappropriate images are found on the computer during routine maintenance work:

1. Do not touch the keyboard or mouse.

2. Do not take any advice from the user.

3. Make a note of what is visible on the screen.

4. Power off the computer by removing the power cable from the unit. Pull out any other cables e.g. mouse, network etc.

5. Carefully remove the equipment, make an inventory of what's been seized and record unique identifiers. Get the inventory independently signed and verified.

6. Ensure that all items have signed and completed labels attached in order to preserve continuity of evidence. The labels should describe the type, model, serial number etc of the equipment.

7. Make detailed notes of all actions taken in relation to the computer equipment on the attached pro-forma.

8. The computer and related equipment must be stored in a secure location until collected.

9. The incident and action taken should immediately be reported to the IT Manager within Children and Young Peoples Services (01942 486063) and they will make arrangements for a forensic examination of the computer.

10. Further advice should be obtained from Corporate Personnel Services.

In addition to the above, for security and accountability reasons, each user of the computer must have an individual user account and password. In the event of inappropriate use of the computer this will enable the investigator to quickly identify the individual responsible. If you are unsure how to create user accounts you should seek advice from IT Officers in Children and Young Peoples' Services (01942 486072).

Investigation Checklist	
Identifying Officer.	Print Name: Job Title: Signature:
How Suspicions Raised: e.g. Routine Maintenance, allegation	
Allegation Against	
Date and Time Identified:	Date: Time:
All Officers who have handled the computer following suspicion aroused:	

Action Checklist		
1	Is the computer switched on? - If not then do not switch on or open lid - Battery removed?	Yes / No Yes / No
2	If computer switched on, do not touch the key board or mouse. - What is visible on the screen?	
3	Power off the computer by removing the power cable / battery direct from the computer	Yes / No
4	Inventory of equipment seized, i.e. computer make, model, serial number, any other peripheral attached. (e.g. floppy disks, pen drives, digital camera etc	Inventory Make: Model: Serial Number: Other Items
5	Inventory independently signed and verified.	Signature Independent Officer Date & Time
6	Labels attached to all items on inventory (signed and dated)	Yes / No
7	User ID and any passwords obtained from user **Note:** There may be more than 1 password for log on and / or protected documents.	Yes / No User ID: Passwords:
8	Incident reported to I.C.T. Manager within Children and Young People's Services	Date & time: Reported To:

Appendix 5

Network Induction Programme
The safe and secure use of the internet and education intranet / VLN requires all staff and pupils to be aware of the potential and dangers associated with on-line access. All users must behave in a responsible manner at all times. To meet these requirements, appropriate training must be undertaken before access permission is granted.

Pupils: (ICT & Technical Staff responsibility)

- All pupils must have the acceptable use policy explained. They must agree to this and along with their parents sign a copy of the policy.

Staff: (Assistant Head: Staff Development).
The Network induction programme for all users should include the following

- information about roles, responsibilities and procedures
- an introduction to the network
- an explanation of the acceptable use policy and its implications
- procedures for managing incidents of inappropriate use
- the allocation of user name and password
- email and Internet access procedures
- guidelines on electronic publishing, including the requirements of the Data Protection Act (1998). the Design, Copyright and Patents Act (1988), the Computer Misuse Act (1990) and the Defamation Act (1996)