ICT POLICY

CONTENTS

Heanor Gate Science College is committed to developing the use of ICT throughout the School organisation and to developing the skills and knowledge of both staff, students and the wider community.

ICT is used by students to assist their work and learning, by staff as a support to their teaching and administrative work and by administration staff to provide effective and efficient support for School systems and procedures.

1. ICT ADMINISTRATION AND CURRICULUM

ICT – Administration
ICT will be used wherever possible to assist staff in their roles and responsibilities, to provide data as appropriate and to assist in the management of School systems, e.g. finance, attendance, performance monitoring.

The Headteacher, Assistant Headteacher, ICT Co-ordinator and IT Manager will be responsible for all aspects of ICT administration.

ICT – Curriculum
ICT will be used wherever possible to assist staff and students in their teaching and learning and the ICT Co-ordinator in conjunction with other key staff will be responsible for all the co-ordination of all aspects of ICT in the curriculum in their teaching.

There are a number of ICT facilities located around the School and as the network develops there will be increased access to ICT resources.

- The School operates an open door policy in the school library so that students who identify a need, which requires the use of ICT in the solution of a task, are able to use the resources located there. The ICT suites are only available if a member of staff is present.

- The ICT suites are bookable through the Room Booking system on the internet

- Technician support is available approximately 100% of the working week and can be utilised (with appropriate prior notice to the IT Manager) to assist with the preparation of related materials to assist your teaching of your subject using Information Technology.

- Problems with machines do occur and can be minimised if staff and pupils take care of the resource, use careful time management and planning.

- Those problems requiring more specialised intervention need to be identified immediately to the ICT Support team via the helpdesk (helpdesk@heanorgate.derbyshire.sch.uk) in order that help can be given and the operation of the resource can be managed effectively.

Software and Licensing
- Software used on School ICT resources must solely be that which has been purchased with an accompanying individual or site licence. This means that the software is licensed for use (either unlimited or limited to a number of machines at any one time) on the School site only.

Additional licences may be purchased by the School where colleagues are required to undertake work at home on specific software. The IT Manager in conjunction with the Assistant Headteacher will monitor and authorise all requests for such software.

- Any software purchases should firstly be discussed with the Assistant Headteacher and when the software arrives in School it is registered centrally with the IT Manager for secure storage.

- Software audits will be carried out on a regular basis to ensure no unlicensed software is being used in School. New software is constantly evaluated and installed to:
  1. Prevent programmes from being downloaded from the Internet
  2. Audit all software on network connected machines via the server

  However a rolling programme of audits will continue on stand alone machines and all other equipment.

  Curriculum Co-ordinators who are concerned that unlicensed software might be being used in their area should discuss the matter with the IT Manager.

- Under no circumstances must copies of any software be transferred to or from any off site system unless the appropriate licence has been purchased and software cannot be hired or sold on to another user.

  Installation of software is the responsibility of the Network Manager and person(s) designated by him/her to carry out that task – i.e. the ICT technician.

  Software is continually being updated and a catalogue of titles is being developed; this is available upon request from the ICT Technician.

- CD's etc of purchased software must be given to the IT Manager on receipt and original copies of licences etc will also be kept by the IT Manager.

- The IT Manager will maintain an inventory of software installed and will advise the appropriate staff, if additional licences need to be purchased. ***This inventory will be reviewed annually by the IT Manager and Assistant Head, signed and dated and retained as evidence of its occurrence and to provide an audit trail***

Security and Inventories

- All computers and associated items will be security marked by the ICT Technician wherever possible. An additional identification mark will also be added to the computers to facilitate the monitoring of individual machines.

- Items should be entered on Curriculum Area inventories as appropriate as well as the Whole School ICT inventory maintained by the ICT Systems Staff. Where possible serial numbers should be recorded for all items.

- The Whole School ICT inventory will provide an overview of all resources within the School and provide a profile of each machine.

Insurance

- The School has insurance to cover the theft of hardware and software from the premises only.

- All staff and students are encouraged to adopt practices which will encourage good security of rooms and equipment.

- Staff wishing to continue curriculum development or professional development by making use of School owned systems outside School hours and off the premises should first discuss the matter with the School Business Manager and complete the personal off site use form available from the School Business Manager.

- Colleagues are advised to check car and home insurance policies to ensure they are adequately covered for any loss or damage prior to using personal items at home.

Damage, Repairs and Virus Protection

- Any staff member detecting any damage or malfunction should report it directly to the helpdesk as soon as it has been detected.

- Memory Sticks / Flash Sticks / USB Keys etc brought into the School must be checked for viruses on designated machines before being used on School systems.

- Every ICT user, member of staff and student has a responsibility to the whole ICT user community.

- Appropriate virus checking software is installed on all workstations in school and all students and staff should ensure disks etc are virus checked before using them on any School computer.

Authorisation and Access

- Levels of access will be established for different users on the various networks and systems operating in School.

- Responsibility for maintaining and monitoring access and authorisation will be as follows:

School Network	IT Manager in consultation with Asst. Headteacher.
Broadband connections	IT Manager
Administration Network	IT Manager in consultation with Asst. Headteacher.
SIMS.net	IT Manager in consultation with School Business Manager

- All access and authorisations will be limited to nominated personnel and details of passwords and other secure information will be kept by the IT Manager as appropriate.

- All staff will follow established ICT guidelines on using passwords effectively and where other guidelines exist, users will follow those guidelines

- Access to the server is limited to nominated personnel who will be advised on security arrangements for the server rooms.

Computer Security and Data Quality

- As detailed in the school ICT acceptable use policy signed by all students and staff students, staff and governors are not permitted to share passwords under any circumstances

- Students and staff are expected to adhere to the principles of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs & Patents Act 1988 and all other relevant legislation

Use of the Internet

- Internet access will be available to staff and students via all workstations connected to the School and administration network where considered appropriate.

- All members of the School community and visitors to the School are expected to sign and follow the rules laid out in the ICT Acceptable Use Policy

- All use of the Internet by students, staff and other users will be monitored and users will be made aware of the monitoring procedure.

- If students or staff discover unsuitable material the URL and the nature of the content should be reported immediately to either the ICT Co-ordinator, IT Manager, ICT Technician, or the Assistant Headteacher immediately.

- Any unsuitable URL or site with inappropriate links will be blocked using the Openhive webfilter software suite and in appropriate situations reported to Capita as soon as possible

- Students are not allowed to access web forums / web chat although access is permitted to monitored user groups where staff are involved in a specific project, e.g. Gifted and Talented, summer school, robot challenge etc. Staff will discuss the issues relating to the use of web chat to highlight potential dangers as part of the core safeguarding processes

- The School e-mail system is also monitored for inappropriate content and the IT Manager will run regular checks on content.

- The School e-mail is randomly checked by the IT Manager who ensures that e-mails reach their required destination. All e-mails not clearly identified to specific staff will be checked and if necessary referred to the Headteacher.

- Any member of the School community or other School user who, in the opinion of the Headteacher, uses the Internet inappropriately will have appropriate sanctions imposed, and if necessary, disciplinary action carried out against them.

Backing up

The majority of school systems are now centrally managed at George Spencer Academy, and as such, the schools data (HGSC) will be backed up as part of their (GSA) own procedures in accordance with their own policies

Where appropriate, the IT Manager (HGSC) will ensure procedures are in place to recover data in the event of a critical incident or local problem.

For the remaining systems still on site, the IT Manager will ensure that they are backed up on a regular basis and tested to ensure data integrity.

2. E-SAFETY

Introduction
It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This policy document is drawn up to protect all parties; the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Context and Background
The Technologies
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

The Internet – world wide web
E-mail
Instant messaging (often using simple web cams) e.g. Instant messenger
Web based voice and video calling (e.g. Skype)
Online chat rooms
Online discussion forums
Social media (e.g. Facebook)
Blogs and Micro-blogs (e.g. Twitter)
Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
Video broadcasting sites (e.g. YouTube)
Music and video downloading (e.g. iTunes)
Mobile phones with camera and video functionality
Smart phones with e-mail, messaging and internet access
Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

An effective range of technological tools;
Policies and procedures, with clear roles and responsibilities
E-Safety teaching is embedded into the school curriculum and schemes of work

Roles and Responsibilities
e-Safety is recognised as an essential aspect of strategic leadership in this school and the Principal, with the support of Governors, aims to embed safe practices into the culture of the school.

The SLT ensure that the Policy is implemented across the school via the usual school monitoring procedures.

Peter Day is responsible for keeping up to date on all e-Safety issues. Where applicable, these will be communicated to staff.

The Governing Body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials.

Staff should ensure they are familiar with the school e-Safety policy, and ask for clarification where needed. They should sign the ICT Policy agreement annually.

Class teachers should ensure that students are aware of the e-Safety rules, introducing them at the beginning of each new school year.

Students are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school.

Parents are given information about the school's e-safety policy at the admission interview. They are given copies of the student information, and asked to support these rules with their children.

Technical and hardware guidance
School Internet provision
The schools internet feed is provided by Advanced IT Services. Staff and students use Office 365 for email which is sat behind a management system provided by Capita.

Content filter
Advanced IT Services (AITS) uses Smoothwall to filter all content coming in and out of school. As a secondary layer, the school uses Impero Classroom Management to filter the content at a more granular level. With this in place, the IT Dept (and teaching staff) can allow / block content for certain classes and even individuals if necessary. Whilst this filtering technology is robust and classed as "enterprise" software it is still possible for unsuitable material to occasionally get past the filter(s).

All students and staff have been issued with clear guidelines on what to do if this happens and parents will be informed where necessary
Students or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document

Downloading files and applications
The internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment. Therefore, students are not allowed to download any material from the internet unless directed to do so by an appropriate member of staff

Portable storage media
Staff are allowed to use their own portable media storage (USB keys etc). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT administrator

Security and virus protection
The school subscribes to Sophos Antivirus. The software is monitored and updated regularly by the school technical support staff and AITS.
Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Manager.

E-Safety for Students
We believe it is our responsibility to prepare students for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching students to use the ICT effectively and appropriately in all aspects of their education.

Internet access at school by students
Internet access is carefully controlled by teachers according to the age and experience of the students, and the learning objectives being addressed. Students are always actively supervised by an adult when using the internet, and computers with internet access are carefully located so that screens can be seen at all times by all who pass by. The Impero management software also allows the IT Dept and classroom staff to monitor screens remotely, and attempts of filter breaches are flagged.

Access for all students
In line with our inclusion policies across the school we want to ensure that all our students have access to the internet, particularly where this will directly support their learning.

Using the internet for learning
The internet is now an invaluable resource for learning for all of our students and we use it across the curriculum both for researching information and a source of digital learning materials.
Using the internet for learning is now a part of the Computing Curriculum (Sept 2015). We teach all of our students how to find appropriate information on the internet and how to ensure, as far as possible, that they understand who has made this information available and how accurate and truthful it is.

Teachers carefully plan all internet-based teaching to ensure that students are focused and using appropriate and relevant materials
Students are taught how to use search engines and how to evaluate internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary
They are taught how to recognise the difference between commercial and non-commercial websites, and how to investigate the possible authors of web-based materials
They are taught how to carry out simple checks for bias and misinformation
They are taught that web-based resources have similarly copyright status as printed and recorded materials such as books, films and music and that this must be taken into consideration when using them

Teaching safe use of the internet and ICT
We think it is crucial to teach students how to use the internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk

The main aspects of this approach include the following five SMART tips:
Safe – Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online
Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present
Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages
Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation
Tell your parent or carer if someone or something makes you feel uncomfortable or worried

Suitable material
We encourage students to see the internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide students with suggestions for suitable sites across the curriculum, and staff always check the suitability of website before suggesting them to students, or using them in teaching.

Non-education materials
We believe it is better to support students in finding their way around the internet with guidance and positive role modelling rather than restrict internet use to strict curriculum based research. As well as internet material directly related to the curriculum, we encourage students to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home. There is a selection of links to such resources available from on the school website, and in the shared student folders on the school network.

Unsuitable material
Despite the best efforts of the internet provider and school staff, occasionally students may come across something on the internet that they find offensive, unpleasant or distressing. Students are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
The action will include:-

1. Making a note of the website and any other websites linked to it
2. Informing the ICT manager
3. Logging the incident – ICT Incident Log Book in the school office
4. Discussion with the student about the incident, and how to avoid similar experiences in future

Using E-Mail at school
E-mail is valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our students understand the role of e-mail, and how to use it appropriately and effectively.

We teach the use of e-mail as part of our ICT curriculum, and use appropriate students email accounts where necessary
Students are not allowed to access personal e-mail using school internet facilities

Chat, discussion and social networking sites
These forums of electronic communication are used more and more by students out of school and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach students how to use chat rooms safely.

All commercial instant messaging and social networking sites are either blocked or filtered in line with LA guidance, AITS filters and school policies.

Students may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual student names or identifying information will never be used.

Internet-enabled mobile phones and handheld devices
More and more young people have access to sophisticated new internet-enabled devices such as smartphones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the internet and allow pictures and information to be remotely posted to a website or weblog.

Students will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

It is worth highlighting, that if a student has a mobile data plan in place on their device (3G, 4G etc) the school cannot block or filter the content that is transmitted; mobile data is completely independent to the schools wireless system and as such, the school has no mechanism (nor jurisdiction) to block that content.

Cyberbullying – Online bullying and harassment
Online bullying and harassment via instant messaging, mobile phone texting, e-mail and chatrooms are potential problems that can have a serious effect on students. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:
No access to public chat-rooms, Instant Messaging services and bulletin boards
Students are taught how to use the internet safely and responsibly and are given access to guidance and support resources from a variety of sources

We encourage students to discuss any concerns or worries they have about online bullying and harassment with staff and have a range of materials available to support students and their families.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy
Complaints related to child protection are dealt with in accordance with school child protection procedures

Contact details and privacy
As specified elsewhere in this policy, students' personal details, identifying information, images or other sensitive details will never be used for any public internet-based activity unless written permission has been obtained from a parent or legal guardian.

Students are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

School and student website – pictures and student input
As part of the ICT and wider curriculum, students may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Students may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where student websites are published on the wider internet, perhaps as part of a project with another school, organisation etc., then identifying information will be removed and images restricted.

Deliberate misuse of the internet facilities
All students have discussed the rules for using the internet safely and appropriately. These rules should be displayed in each classroom and the ICT suite.

Where a student is found to be using the internet appropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse and any previous misuse.

Sanctions will include:-

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)
Initial warning for class teacher
Banning from out of school hours internet facilities
Reported to the CTL
Letter to the Parent/Carer

Offensive material
Meeting with Parent/Carer to re-sign internet use agreement
Removal of Out of School Hours access to internet
Subsequent incidents will be treated very seriously by the Principal and may result in exclusion and/ or police involvement

How will complaints regarding e-Safety be handled?
It is the duty of the school to ensure that every child in our care is safe and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

International scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school

computer or mobile device. Neither the school, LA or Trust Academy can accept liability for material accessed, or any consequences of internet access.

Staff and students are given information about infringements in use and possible sanctions.

Sanctions available include:-
All incidents will be recorded
Interview/counselling by class teacher, SLT, e-Safety Co-ordinator and Principal
Informing Parent/Carers
Removal of internet or computer access for a period
Referral to LA/Police

Our e-Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal.

Use of the internet and ICT resources by school staff
The internet
Our school understands that the internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion.

We are committed to encouraging and supporting our school staff to make the best use of the internet and all the opportunities it offers to enhance our teaching and supporting learning.

Internet availability
To enable staff to make full use of these important resources, the internet is available in school to all staff for professional use. The school provides an Office 365 email account as well as online versions of Word, Excel etc. Google App accounts are also available where required.

ICT equipment and resources
The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.
Professional use
Staff are expected to model appropriate ICT internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and internet use by our students both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the internet, and to provide students with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need to support or INSET in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

Personal use of the internet and ICT resources
Some equipment (including laptops) is available for loan to staff, with permission from the ICT Manager and Principal. The appropriate forms (available from IT Support) and agreements must be signed.
However, all staff must be aware of the school policy on using school internet and ICT resources for personal use. These are outlined in the staff agreement form below.

Email
We recognise that e-mail is a useful and efficient professional communication tool. To facilitate this staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this e-mail address means that they are representing the school and all communications must reflect this.

E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.

Online discussion groups, bulletin boards and forums, online chat and messaging
We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school and appropriate professional standards should apply to all postings and messages.

Social Networking
The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct Expectations and Agreements.

Data protection and copyright
The school has a Data Protection Policy in place – please see separate documentation for more details.

Staff are aware of this policy and how it relates to internet and ICT use, in particular with regard to student data and photographs, and follow the guidelines as necessary.
Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support students to do the same.

Data Protection Policy
Our school is aware of the data protection law as it affects our use of the internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data protection

Staff and students understand the legal and disciplinary implications of using the internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the internet by members of the school community using the connection provided by the school.

Staff laptop and ICT equipment loans
Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e-Safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of HGSC at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement' before taking the equipment away from the school premises.

3. ACCEPTABLE USE OF ICT, INTERNET & ELECTRONIC COMMUNICATION

Heanor Gate Science College is committed to providing Internet and email facilities to staff where an educational need is established and, to promote staff awareness of the benefits and potential dangers involved. This policy sets out guidelines for employee use.

Infringement of this policy by staff may be regarded as a disciplinary offence and in serious cases, may result in dismissal. Improper use of the Internet or email could bring the School into disrepute and may lead to legal claims against the individual employee and the School.

Guidelines

1. The Principal will authorise use of the Internet or email facilities prior to staff accessing these and will keep a written list of all such authorisations.
2. Ownership of all computer hardware, software and documents lies with the School and the School reserves the right to make appropriate arrangements to monitor, log, record and access all communications at any time without notice.
3. Use of the Internet and email must be for the educational purposes of the School only and the scale of use must be appropriate to those purposes.
4. Staff are required to maintain the good reputation of the School when using the Internet and email and to be aware that these services are open forums subject to public scrutiny.
5. Examples of misuse which contravene this policy and the possible resulting sanctions are:
    i. Personal use of Internet and email may lead to withdrawal of user's rights and/or financial charges being imposed.
    ii. Distributing abusive, discriminatory or defamatory statements may be regarded as serious acts of misconduct and will normally lead to disciplinary action.
    iii. Visiting, downloading or distributing pornographic, obscene, offensive or illegal material may be regarded as gross misconduct and may lead to summary dismissal.
6. Appropriate security must be applied before confidential or sensitive information is sent via the Internet or by email.
7. Staff must not form contracts or vary contractual terms over the Internet unless authorised to do so.
8. Any material imported by Internet or email must be virus-checked and must not infringe copyright.
9. Publication of information on the Internet must only be via the School web site.
10. Where access is gained accidentally to Internet sites that may infringe these guidelines, the ICT Manager and, if appropriate, Principal must be informed immediately.
11. Staff will be required to confirm that they have read and accept the guidelines in this policy.

I have read and accept these guidelines

Signed:	
Name (BLOCK CAPITALS):	
Date:	

4. PASSWORDS

New staff will be issued with passwords for (i) network, (ii) email and (iii) SIMS.net by the IT Manager.

These passwords will be issued through the Head of Department, documentation placed in the appropriate staff pigeonhole, or meeting with the individual.

Network passwords

- Passwords for newly created network accounts will need to be changed upon first logon. This will be requested by the system
- Network passwords are set to expire every 72 days. If the password is not reset within 20 days the relevant account is automatically disabled. Users will need to contact the ICT Support team to have the account re-enabled.
- When logging on, if an incorrect password is entered three consecutive times, the relevant account will be disabled. Users will need to call ICT Support team to re-enable this account.
- Password must be at least four characters in length.
- Staff and students can change their password at any time by simultaneously pressing the CTRL ALT DELETE keys and selecting the "change password" option. Doing this will also reset the 72 day expiry time.

SIMS.net passwords

- Passwords for SIMS.net accounts will need to be changed at first use. This will be requested by the system.
- The passwords in SIMS.net do not have an expiry time. It is therefore recommended that when the password for the network expires (point 2.1.1), the user initiates a SIMS.net password change by ticking the box on the SIMS.net logon screen

Email passwords

- Email passwords are not set by the ICT Support team in school; they are initially provided by Capita but thereafter, can be changed either by the ICT Support team or by the user (by clicking the SST icon on the email home page)
- There is no expiry time on email passwords. It is once again recommended, that at the time of the network password change, the email password is also changed

Password Guidelines

- Whilst it would be easier for users to maintain the same password for (i) network, (ii) email and (iii) SIMS.net, staff are encouraged to make the passwords significantly different from one another – *if the same password existed for all services, the potential for data loss significantly increases.*
- The password must not be the same as the user ID.
- The password must not include the first, middle, or last name of the user.
- Passwords must not be shared with anyone (the ICT Support team may ask for this when resolving a problem but will get you to change it once sorted)
- Never communicate a password by telephone, e-mail or instant messaging
- Passwords must not be written down.
- For systems *other* than (i) network, (ii) email and (iii) SIMS.net, please use the same principles.
- Website passwords are only secure if used on websites beginning with http**s**://.

- All use of the Heanor Gate Science College systems and account(s) are assumed to be performed by the person assigned to that account. Account owners are held responsible for all activities and content associated with their accounts.
- Failure to conform to these requirements may lead to suspension of account privileges or other action as indicated by the Acceptable Use Policy (ICT) and other school policies.

Password Best Practices

- Use numbers in your passwords. A good method is to substitute the letters "I", "O" and "S" with the numbers "1 (one)", "0 (zero)" and "5 (five)". An example of this would be to take the word "position" – using the method detailed, the password becomes "p051t10n"
- Try not to use a common dictionary word, someone's name, a string of numbers, or your User ID.
- Pick something that is memorable to you but at the same time try and ensure that no-one else can guess what it is. Making a password completely random only strengthens security
- If permitted by the system / application, use non-alphanumeric characters eg \ +, %, £ etc
- Never keep a password blank or set as "password"
- Always be careful to log off before leaving a computer unattended
- Always change passwords whenever there is suspicion they may have been compromised

Support

- Individuals who forget their password or need assistance should contact ICT Service Desk / IT Support staff.