The King’s School Academy Trust

Use of New Technologies, Data Protection, Computer Security and Cyberbullying Policy

The King’s School
Cadhay Lane
Ottery-St-Mary
Devon
EX11 1RA

Policy Change Control

Policy Owner	DHT Curriculum
Approved By	Resources Committee
Date of Last Approval	26/09/2017
Next Revision Due	September 2020

Date	Version	Person	Change / Action
30/01/2014	1.0	Governors	Adoption of Policy
02/05/2017	1.1	LOE	Update to Template and Format
19/09/2017	1.2	DGW	No changes
26/09/2017	1.2	Governors	Presented to Governors for Approval

1.0 Data Protection Policy

1.1 Introduction

The Data Protection Act 1998 came into force on 1st March 2000. It sets out what can and what cannot be done with personal data that is information about living individuals. The King's School is placed under a legal obligation to comply with the provisions of this Act.

1.2 Commitment to the Protection of Personal Information

The King's School needs to collect and use certain types of information about people with whom it deals in order to operate effectively. These include pupils, parents, guardians, staff, governors, suppliers and others with whom it communicates. In addition, it is required by law to collect and use certain types of information to comply with the requirements of government departments.

This personal information must be dealt with properly and securely regardless of what method is used for its collection, recording or use – whether this is paper, a computer system or any other material. There are safeguards to ensure that the processing of such information is carried out in a proper fashion and these are contained in the Act.

This policy does not seek to convey the whole legislation to its readers, rather to acquaint them with the main provisions and to demonstrate that The King's School has a commitment to those provisions. Further detailed information relating to data protection legislation can be obtained from the Information Commissioner's Office website – www.ico.gov.uk

The King's School regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions and to maintaining confidence between those with whom we deal and ourselves. We ensure that our school treats personal information lawfully and fairly.

1.3 Our Data Protection Standards

The King's School will, through appropriate management and adherence to agreed procedures:

- Observe fully the conditions relating to the fair collection and use of personal information
- Meet its legal obligations to specify the purposes for which the information is used
- Collect and process appropriate information but only that which is necessary to its operational needs or meet its legal requirements
- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held and to ensure that it will be disposed of when no longer required with due regard for its sensitivity.
- Ensure that the rights of people about whom information is held can be exercised. These include the right to be informed that processing is being undertaken, the right to access one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong.
- Take appropriate technical and organisational measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.

1.4 Management Arrangements

The King's School will ensure that:

- Someone is nominated to hold specific responsibility for data protection within the school.
- Everyone managing and handling personal information understands that they are responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised

- Anyone wanting to make enquiries about handling personal information knows what to do
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated.

2.0 Information Security Policy

2.1 Introduction

The school's investment in the acquisition, storage and use of electronic and paper based information exists primarily to help provide the effective delivery of its services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment.

The school is committed to achieving policy requirements through an Information Security process. To actively demonstrate this, the School has issued a Commitment Statement which provides assurance to pupils, parents, governors and staff that sound and secure measures are in place to protect the confidentiality, integrity and availability of their information.

2.2 Objective

The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

2.3 Policy

The purpose of this policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

The key aims of the policy are to ensure that:

- information is protected from unauthorised access
- confidentiality of personal or sensitive information is assured
- integrity of information is maintained
- information is disposed of in a timely, appropriate and secure manner
- legislative requirements and school policy and practices are observed
- business continuity plans are produced, maintained and tested
- information security training is available to all school staff
- appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

2.4 Supporting framework

In order to achieve this, the school will develop and maintain information security standards. Procedures, working practices and protocols will be developed to support this policy. Examples of measures to achieve the above are physical security, virus control and the use of passwords for access control. The development of any new system will include information security analysis and requirements as part of the initial specification.

2.5 Responsibilities

The school's Head Teacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that staff they manage also adhere to the standards.

2.6 Implementation

This policy will be made available to all pupils, parents, guardians, staff (whether permanent or temporary) and governors.

2.7 Information Commitment Statement

Your Information - Our Commitment

- ***The King's School holds a great deal of information, much of which is confidential. This may be information about:***

  - ***our pupils***
  - ***our pupil's parents or guardians***
  - ***our governors***
  - ***our teachers and other staff***

If we hold information about you, we wish to assure you that we are processing the information fairly and lawfully and that we will inform you of the purposes for which we require the information when you supply it to us.

-

In particular:

When we collect information

- we will only collect information that is necessary for what we do
- we will be fair in the way we collect information about you
- we will tell you who we are and what we intend to do with the information about you
- where practicable, we will collect information which relates to you directly from you
- if we collect information about you from someone else we will, wherever possible, make sure you know that we have done this

When we use and disclose information about you

- we will only use or disclose your information for legitimate purposes about which you have been told unless we are required to do otherwise for legal reasons

Information quality

- we will ensure that information about you is accurate and up to date when we collect or use it. You can help us to achieve this by keeping us informed of any changes to the information we hold about you

Information security

- we will keep information about you secure
- we will protect your information against unauthorised use, damage, loss and theft

Retention

- we will hold information about you for as long as is necessary but, subject to any statutory retention periods, we will ensure that the information is disposed of in a secure and proper manner when it is no longer needed

Openness

- we will be open with you about what kinds of information we hold and what we do with it

Access and correction

- wherever possible, we will let you see the information we hold about you (should you wish) and correct it if it is wrong

In general:

- we will comply with the provisions of the Data Protection Act 1998 and any subsequent legislation relating to information handling and privacy. We will achieve this through the school's Information Security and Data Protection Policies supported by proper working practices and procedures.

3.0 Computer Security/SIMS User Policy

3.1 Introduction

The school has a one network system meaning all staff have access to the SIMS data base. Some staff will be familiar with SIMS and some will need training to access the information they need. The School Network and SIMS hold huge amounts of confidential and sometimes sensitive data about students and of course in some programmes staff information (access to SIMS is not open access).

3.2 Objective

To keep this information secure and confidential and to maintain our legal obligations under the data protection act we must have in place a clear policy to which all staff users must sign. The security of The School Network and SIMS relies on three main aspects: "clear desks", passwords and public\shared folders.

3.3 Policy

The purpose of this policy is to ensure access to the school's confidential information is limited only to those who need it.

CLEAR DESKS

- If a computer is to be left unattended especially when SIMS is not closed then it MUST be left locked
- Computers must never be open with SIMS running in a place where students can view the screen

PASSWORDS

- Passwords MUST be at least 8 characters long.
- Users must change their password in the first week of every half term
- Password should follow the three of four rule.

PUBLIC\SHARED Folders

- Files students must not access cannot be placed in the U Drive (This includes student photos)
- Files which are inappropriate for all staff (an example is personnel files) in your "My documents" folder\H:\ drive or an access restricted folder/drive (IT support will set this up for you)
- Files which are not suitable to be viewed by students must not be kept on any computers C:\ drive.

3.4 Supporting framework

In order to achieve this, there is a form every member of staff must read and agree to (Appendix 3). The network is set up to enforce a password reset every three months.

3.5 Responsibilities

The school's Head Teacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that staff they manage also adhere to the standards.

3.6 Implementation

This policy will be made available to all pupils, parents, guardians, staff (whether permanent or temporary) and governors.

4.0 Cyber Bullying and use of New Technologies Policy

4.1 What is cyberbullying?

"Cyberbullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."

Seven categories of cyberbullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort.
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified.
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Chat room bullying involves sending menacing or upsetting responses to children or young people when they are in a web-based chat room.
- Bullying through instant messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online.
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyberbullying.

4.2 What can schools do about it?

While other forms of bullying remain prevalent, cyberbullying is already a significant issue for many young people. The King’s School recognise that staff, parents and young people need to work together to prevent this and to tackle it whenever it occurs.

School Governors, Head teachers and schools have a duty to ensure that: bullying via mobile phone or the Internet is included in their mandatory anti-bullying policies, that these policies are regularly updated, and that teachers have sufficient knowledge to deal with cyberbullying in school.

The King’s School ensures that:

- the curriculum teaches pupils about the risks of new communications technologies, the consequences of their misuse, and how to use them safely including personal rights
- all e-communications used on the school site or as part of school activities off-site are monitored
- clear policies are set about the use of mobile phones at school and at other times when young people are under the school's authority. No mobile phones with cameras will be seen or heard on the school site. If a phone is seen or heard it will be confiscated and locked in the school safe until parents are able to collect it.
- Internet blocking technologies are continually updated and harmful sites blocked
- they work with pupils and parents to make sure new communications technologies are used safely, taking account of local and national guidance and good practice
- security systems are in place to prevent images and information about pupils and staff being accessed improperly from outside school
- they work with police and other partners on managing cyberbullying.
- A record of the incident will be kept.

4.3 ICT and Mobile Phone Policy

If a cyberbullying incident directed at a child occurs using e-mail or mobile phone technology, either inside or outside school time, The King’s School will take the following steps:

- Advise the child not to respond to the message
- Refer to relevant policies, e.g. e-safety/student acceptable use (appendix x) , anti-bullying and PSHE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the sender’s e-mail service provider

- Notify parents of the children involved
- Consider delivering a parent workshop for the school community
- Consider informing the police depending on the severity or repetitious nature of the offence. The school recognises that some cyberbullying activities could be a criminal offence under a range of different laws including: the Protection from Harassment Act 1997; the Malicious Communication Act 1988; section 127 of the Communications Act 2003 and the Public Order Act 1986

If malicious or threatening comments are posted on an Internet site or Social Networking Site about a pupil of member of staff, The King's School **will also:**

- Inform and request that the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to www.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform the police as appropriate.

4.4 Working with Parents

The King's School has developed a home-school agreement that includes clear statements about e-communications. The school seeks to regularly update parents on:

- What to do if problems arise
- E-communication standards and practices in school
- What's being taught in the curriculum
- Supporting parents and pupils if cyberbullying occurs by:
    - Assessing the harm done
    - Identifying those involved
    - Taking steps to repair harm and to prevent recurrence

4.5 Code of Conduct

The King's School has developed a code of conduct with our pupils. This is available in IT rooms/classrooms etc.

EXEMPLAR CODE OF CONDUCT

- Always respect others - be careful what you say online and what images you send
- THINK before you send. Whatever you send could be made public very quickly and could stay online forever
- Treat your password like your toothbrush – keep it to yourself. Only give your mobile phone number or personal website address to trusted friends
- Serious bullying should be reported to the police – for example threats of a physical or sexual nature
- If you can, make a note of the time and date bullying messages or images were sent and note any details about the sender
- Don't retaliate or reply
- Keep and save any offending emails, text messages, images or online conversations

Make sure you tell:

- An adult you trust or call a helpline like Childline on 0800 1111 in confidence or CEOPS www.ceop.gov.uk/reportabuse/index.asp

- The service provider. Check the mobile phone company or internet provider. They may be able to track the bully down

- Your school. Your tutor, Head of House or Student Support can help you.

4.6 CYBERBULLYING RESOURCES FOR SCHOOLS

www.childnet-int.org has a DVD for secondary schools about keeping safe in online chat rooms.. Order at www.childnet-int.org/order.
Childnet International also advises on Internet safety and has a range of leaflets for children and parents in a number of languages, including Hindi, Punjabi and Maltese.

www.cybersmartcurriculum.org has lesson plans for teachers on dealing with online bullies.

There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org The Kidscape booklet 'Don't Bully Me!' gives advice to primary school children on what to do if they are bullied.

www.wiredsafety.org has some useful tips.

Stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting by making them believe the number's changed. To find out how to do this, visit www.wiredsafety.org.
If the bullying persists, you can change your phone number. Ask your mobile service provider (such as Orange, O2, Vodafone or T-Mobile).

Secondary school teachers can download an information pack from www.stoptextbully.com including a classroom quiz, poster and top tips to help tackle cyberbullying. It is an interactive website that helps young people tackle mobile phone and online bullying and prevent it ever happening to them. There's advice for pupils, parents, carers and teachers, along with a fun quiz that highlights the issues.

Child Exploitation and Online Protection Centre (CEOP)

Set up by the Government, the CEOP website helps adults get to grips with new and emerging technologies popular with young people. It includes advice on how to report cyberbullying, sexual abuse on line and the dangers of viruses

Don't suffer in silence

This Government website has a short anti-bullying video featuring stars like Rio Ferdinand and the Sugababes, a downloadable charter and advice for pupils, teachers and parents.

Thinkuknow.co.uk
Information from the Child Exploitation and Online Protection Centre on how to stay safe online. It includes details of the CEOP training courses. It provides interactive resources for KS1-KS4, teachers and parents

Virtual Global Taskforce (VGT)

Made up of police forces around the world, working together to fight online child abuse. The site includes advice, information and support for adults and children.

-
- http://www.kidsmart.org.uk/ has some useful tips.
-
- http://www.teach-ict.com/ks3/internet_safety/staying_safe/stayingsafe1.htm also has some useful tips.
-

Appendix 1 - PRIVACY NOTICE
School Workforce: those employed or otherwise engaged to work at a school

Privacy Notice - Data Protection Act 1998

We, The King's School, are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the school about those employed or otherwise engaged to work at the school. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modeling and planning;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.

We are required by law to pass on some of this data to:

- the Department for Education (DfE)
- HMRC
- pension providers

If you require more information about how the DfE store and use this data please go to the following websites:

- http://www.education.gov.uk/schools/adminandfinance/schooladmin/a0077963/what-the-department-does-with-school-workforce-data

- http://www.hmrc.gov.uk/leaflets/dp-fs1.htm#3

If you are unable to access these websites, please contact the DfE as follows:

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT

Website: www.education.gov.uk
Email: info@education.gsi.gov.uk
Telephone: 0370 000 2288.

Appendix 2
PRIVACY NOTICE For Pupils in Schools

Privacy Notice - Data Protection Act 1998

We, The King's School, are a data controller for the purposes of the Data Protection Act. We collect personal information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data to:

- Support your learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well we are doing.

Information about you that we hold includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs you may have and relevant medical information. If you are enrolling for post 14 qualifications the Learning Records Service will give us your unique learner number (ULN) and may also give us details about your learning or qualifications.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the Careers South West service for young people aged 13 to 19 in England. We must provide the names and addresses of you and your parent(s), and any further information relevant to the support services' role.

However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, addresses and your date of birth be passed to the support service. This right transfers to you on your 16th birthday. Please tell Mr Garrick if you wish to opt out of this arrangement. For more information about young people's services, please go to the National Careers Service page at https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx

We will not give information about you to anyone without your consent unless the law and our policies allow us to.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use of the LA. If you want to receive a copy of the information about you that we hold or share, please contact Mr Garrick. If you need more information about how the LA and DfE store and use your information, then please go to the following websites:

http://www.devon.gov.uk/j4s-privacynotice-whatladoes.pdf or

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you cannot access these websites, please contact the LA or DfE as follows:

- Information Governance Manager

Customer Relations & Information Governance Team
Room 120
County Hall
Exeter, EX2 4QD
Telephone: 01392 383445 E-mail: dpoffice@devon.gov.uk

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: www.education.gov.uk
  Telephone: 0370 000 2288Email: http://www.education.gov.uk/help/contactus

Appendix 3
Student ICT Acceptable Use Policy

I agree that I will:

- be responsible for all the ICT activity in my area.
- keep my account secure and not give my username and password to anybody.
- not attempt to operate a computer using another person's login username and password and/or access another person's files.
- not attempt to gain unauthorised access to any part of the King’s School network that is not available from my personal logon.
- not attempt to use or load programmes, files, tools or shortcuts to gain access to either the workstations or any other part of the network.
- Immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.
- only visit websites which are appropriate to my work.
- not visit websites that contain unsuitable material.
- not attempt to set-up or use any proxy by-pass software, or employ any other means in order to by-pass the student/school internet filter.
- not meet anyone whom I have made contact with on the internet without discussing this first with my parents/carers.
- take part in e-safety lessons and take personal responsibility for my awareness of the risks and opportunities posed by technology.
- report any student who is not following this policy and/or e-safety guidelines and inform a teacher/parent/carer.
- Think! Before I post anything on the internet, I understand that anything that I put on the internet can be copied and if this happens it cannot be removed.
- not take information from the internet and pass it off as my own work (plagiarism).
- be aware that any email going out from the school will carry the school address and so represents myself and the school.
- Not email external email addresses with permission of a member of staff.
- Not use external email\social network services in school. In exceptional circumstances use of external these services must be done in direct supervision of a member of staff.
- not include in any email any material or language that is inappropriate.
- always keep my personal details private.
- not use any device or technology for bullying or harassment in any form. (A device includes but is not limited to: phone, computer, pager and includes devices not owned by the school)
- only copy appropriate pictures or text into my area on the network.
- not copy any other type of file to the network without express permission. For example software, games, music, videos, screen savers etc.
- not store files anywhere in the school network that are not relevant to my school work.
- use the technology legally
- not connect any personal equipment to the network without the Network Manager’s permission. (this includes but is not limited to laptops and mp3 players)
- ask a teacher before I print out any information from the internet and will make sure I know the number of pages being printed before I do so.
- respect the ICT equipment. I will not vandalise or abuse the equipment. I will put unwanted printouts into the recycling bin. I will leave my working area tidy, and I will not eat or drink in the ICT rooms nor will I take food and drink into the ICT rooms.
- not use a computer where a member of staff has not given their permission.
- abide by The Code of Conduct for the ICT Rooms displayed in each computer room.

In order for The King’s School to meet legal requirements we now have to make it clear that all student’s emails, files and web use will be logged and scanned for your own protection.
This policy may be updated or modified at any time should the school deem it necessary.
The school reserves the right to review a student's access to either the internet or the school network removed or other appropriate action being taken if the AUP has been breached.

Student:
I understand and will abide by the conditions of this AUP. I understand that any violations of the above conditions may result in disciplinary action, the revoking of my user account, and any other appropriate action. I also agree to report any misuse of the information systems to The King's School teachers or Administrative staff.

Student Name (please print):_______________________________________

Tutor Group: ____

Signature:____ Date:___/___/____

Parent/Carer:

As the parent or carer of this student, I have read the ICT AUP and understand that student access to technology resources at The Kings School is intended for educational purposes. I understand that it is impossible for The King's school to restrict access to all controversial materials. If I become aware of any misuse of the information systems I will contact The King's School to allow them to prevent a reoccurrence. (Misuse can come in many forms, but can be viewed as any network use that indicates or suggests pornography, unethical or illegal solicitation, racism, sexism, inappropriate language).

I hereby give my permission for my child to use the wide range of electronic services available to her/him while attending The King's School.

Parent or Guardian Name (please print): ________________________________

Signature:____ Date:___/___/____

Appendix 4
Computer Security/SIMS User Policy

The school runs a one network system so that staff can have "read only" access to the SIMS data base. Some staff will be familiar with SIMS and some will need training to access the information they need. The School Network and SIMS hold huge amounts of confidential and sometimes sensitive data about students and of course in some programmes staff information (access to SIMS **will not** be open access).

To keep this information secure and confidential and to maintain our legal obligations under the data protection act we must have in place a clear policy to which all staff users must sign. The security of The School Network and SIMS relies on two main aspects: "clear desks" and passwords.

CLEAR DESKS

- Computers must never be left unattended with the SIMS programme open.
- If a computer is to be left unattended especially when SIMS is not closed then it MUST be left locked
- Computers must never be open with SIMS running in a place where students can view the screen (Care MUST also be taken with computers connected to projectors)

PASSWORDS

- Your password MUST be at least 8 characters long.
- Change your password in the first week of every half term
- Use a different unique password each time you change the password.
- Your password should have three of these four following features:
- Uppercase letters
- Lowercase letters
- Numerals
- Other characters (such as "!&* and %)

To make your password more secure:

- Put your password in inverted commas
- Add a memorable date at the end
- Start or finish the password with a capital letter

PUBLIC\SHARED Folders

- Files students must not access cannot be placed in the U Drive (This includes student photos)
- Files which are inappropriate for all staff (an example is personnel files) in your "My documents" folder\H:\ drive or an access restricted folder/drive (IT support will set this up for you)
- Files which are not suitable to be viewed by students must not be kept on any computers C:\ drive.

This helps to make the information we hold about students, their parents or guardians and their family details far more secure.

A password is very important
It is vital to your electronic identity. Choose one that is easy for you to remember but difficult for others to guess.

Much of our information is sensitive
It often concerns vulnerable children. We must make sure that this is held securely and safely.

It's not all about technology
Safeguarding school information is an important issue. You must play your part by making sure that your password is known only to you. If others gain access, the safety of information held will be put at risk.

To Lock your Computer
Press and hold together CTRL + ALT + DEL and click Lock computer

How to change your Windows Password

Note: The School Network will prompt you to change your password at the beginning of each term. It is recommended that you change your password before it expires, expired passwords cannot access emails or remote resources. If you forget your password, IT Services can help you to reset it.

1. Log on to the workstation
2. Wait for the Windows Desktop to be displayed
3. Press and hold together **CTRL** + **ALT** + **DEL** (the screen will blank and a dialog box will be displayed)
4. Choose the "**Change Password**" button
5. Type in your **old password** in the box provided
6. Type in your **new password** and confirm the password in the last 2 boxes
7. Press **OK**, Windows will confirm that the password has been accepted
8. Repeat the process on all the other computers that you use

How to change your SIMS Terminal Server Password
Note: The SIMS Terminal Server will automatically prompt you to change your password after 40 days since the last change. It is recommended that you change your password before a holiday. If you have forgotten your SIMS password, please speak with T Hall

- Log on to the SIMS Terminal Server
- Wait for SIMS .net to load
- Press and hold together **CTRL** + **ALT** + **END** (or **ALT Gr** + **END** for two fingered typists)
- Choose the "**Change Password**" button
- Type in your **old password** in the box provided
- Type in your **new password** and confirm the password
- Press **OK**, the Terminal Server will confirm that the password has been accepted

After 5 incorrect attempts the account is locked for 30 minutes, this prevents someone from constantly trying to guess the password. In the case of genuine error and the user is remote the user can attempt to type the correct password 30 minutes later.
King's School NETWORK/SIMS USER Policy

✂ ____

I have read and understand the King's School SIMS user policy. I agree to abide by the procedures and systems laid out in the policy.

I do intend to access the SIMS data base to obtain information regarding students

I do not intend to access the SIMS data base (I will inform T. Hall if I wish to change this decision)

(please delete as appropriate)

Signed: ______________________________ Date: ____________

Name:______________________________

Please return to T. Hall