OLDFIELD SCHOOL

ICT POLICY

Last Review:	Jul 2016
Committee:	SLT
Date Ratified:	01/07/2016
Next Review:	Jul 2018

1 Introduction

Education provides students with opportunities and these are greatly increased by the use of ICT. The ability to select appropriate ICT and to use it effectively enhances the learning process at all levels and across a wide range of activities. The inclusion of ICT in the curriculum also assists students to become knowledgeable about the nature of information, comfortable with new technology and able to exploit its potential.

This policy must be used in conjunction with other related policies, namely the E-safety Policy, the Data Protection and Information Security Policy and the Mobile Phone and Other Personal Electronic Devices Policy. E-safety is also referenced in the Safeguarding Children and Child Protection Policy.

2 Objectives and Targets

This policy is aimed at ensuring ICT use at Oldfield School is fit for purpose, efficient and appropriate. It applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

3 ICT Entitlement

3.1 Students are made aware through assemblies, lessons, house or year group meetings, and through the Acceptable Use Guidance, that ICT has many forms and applications and that it is used as a tool to support and enhance teaching and learning.

3.2 The school provides students with meaningful, appropriate experiences in some or all of the following areas:

- handling a computer;
- word processing;
- desk top publishing (DTP);
- information handling (databases);
- manipulation and display of values (spreadsheets);
- simulation and modelling;
- design and manipulation of shapes, data and functions (design and graphics packages);
- web-site creation;
- communications;

- computer programming;
- data logging activities;
- control technology;
- music making and recording;
- problem solving approaches to learning;
- research using a wide range of sources such as CD ROMs and the Internet and Intranet.

3.3 The school provides access to ICT facilities outside of normal lesson times, such as at lunch time, or after school. These sessions may be supervised by a teacher or technician, in which specialist support is available; or unsupervised, for private study.

4 Organisation – Roles and Responsibilities

4.1 The Headteacher

4.1.1 is responsible and accountable to the Governors for implementing the school's Information and Communications Technology Policy;

4.1.2 is responsible for ensuring that the ICT Policy is understood and complied with at all levels;

4.1.3 ensures that matters relating to ICT and its delivery are monitored and reviewed regularly;

4.1.4 delegates the day-to-day management of specified ICT matters to the Business Development and Finance Director.

4.2 Business Development and Finance Director

4.2.1 is responsible to the Headteacher for the day-to-day management of whole school ICT;

4.2.2 is responsible for ensuring that all new, amended or updated materials, regarding ICT matters, are brought to the attention of the relevant personnel immediately upon receipt;

4.2.3 liaises with the Head of ICT and Computing, Heads of Faculty, Curriculum Co-ordinators and staff in charge of subjects to ensure that ICT delivery, assessment, recording and reporting procedures and arrangements are adhered to, consistently and effectively, and are in line with current requirements for the implementation of ICT Across The Curriculum (ICTAC);

4.2.4 must be conversant with current statutory requirements relating to developments in ICT and Computing;

4.2.5 must provide the Headteacher with the information required for monitoring and review purposes;

4.2.6 is responsible for ensuring that matters relating to whole school ICT are included in the School’s Development Plan.

4.3 Head of ICT and Computing

4.3.1 is responsible and accountable to the Head of Faculty (Mathematics) for all matters relating to the provision and delivery of the ICT and Computing curriculum;

4.3.2 is responsible for leading ICT practice within the ICT and Computing Department and for informing faculty colleagues of developments;

4.3.3 must be aware of relevant regulations and other requirements appropriate to the ICT and Computing subject area;

4.3.4 is responsible for the implementation of ICT Policy for the ICT and Computing Department; bringing it to the attention of staff in the department.

4.3.5 must ensure that department staff are familiar with the relevant software packages and identify staff INSET requirements.

4.3.6 must ensure that the recording system for progress in ICT and Computing meets the school's requirements.

4.3.7 is responsible for ensuring that matters relating to ICT and Computing as a subject area are included in the School’s Development Plan

4.4 Heads of Faculty and Subject Leaders

4.4.1 are responsible and accountable to the Headteacher and Assistant Headteacher, and, if applicable, their Head of Faculty, for all matters relating to the provision and delivery of ICT opportunities within their faculty or subject;

4.4.2 are responsible for leading ICT practice within their faculty or subject and for informing faculty colleagues of developments;

4.4.3 must be aware of relevant regulations and other requirements appropriate to their specialist areas;

4.4.4 are responsible for the implementation of the ICT Policy within their faculty or subject, defining the organisation and procedures, and bringing it to the attention of staff in their faculty.

4.4.5 must ensure that departmental schemes of work indicate ICT content addressed;

4.4.6 must ensure that ICT opportunities are clearly identified in the schemes of work;

4.4.7 must ensure that staff are familiar with the relevant software packages and identify staff INSET requirements.

4.5 Teachers

4.5.1 are responsible to their Heads of Faculty or Subject Leaders for the implementation of the school's ICT Policy, in the performance of their duties;

4.5.2 must be familiar with the school's policy and with any procedures, arrangements and practices relating to their department/subject;

4.5.3 must conform to the responsibilities as laid down in their own faculty/subject procedures.

4.6 Network Manager

4.6.1 is responsible to the Business Development and Finance Director for managing and controlling all aspects of the installation, configuration, operation, maintenance and development of the school’s ICT hardware, software and network infrastructure.

4.6.2 develop and implement an effective backup and disaster recovery strategy to ensure against loss of data through error, abuse, malfunction or disaster.

4.6.3 ensure the efficient running of all servers, computers and peripherals throughout the school.

4.6.4 act as point of contact regarding all technical issues with manufacturers, suppliers, ISP and external support organistations.

4.6.5 ensure all ICT equipment and workstations meet the requirements of health and safety legislation and are maintained in a secure, clean and safe manner.

4.6.6 maintain all necessary records and documentation including network maps and inventories and details of licences, warranties and equipment checks as necessary.

4.6.7 support the Business Development and Finance Director in the implementation and upkeep of management systems, offering staff guidance and assisting the Business Development and Finance Director in the insertion of new data into these systems.

4.6.8. resolve ICT problems reported by staff, referring to external organisations where necessary and keeping staff informed of progress with solutions.

4.7 ICT Technicians

4.7.1 are responsible to the Network Manager for the first line maintenance of all the network related or standalone computer hardware within the school;

4.7.2 must be familiar with all network operating systems and main applications software currently in use in the school;

4.7.3 liaise with the various ‘Online Support’ personnel and technical services agencies to solve equipment problems that they are unable to solve internally, ensuring that as much equipment as possible is operational at any one time;

4.7.4 liaise with Heads of Faculty or their delegated representatives with responsibility for their computer equipment, with respect to maintenance issues;

4.7.5 assist with the training of teaching staff as required in aspects of network and peripherals operation, the use of the common software applications and problems associated with classes logging on to the system;

4.7.6 support lessons in ICT network rooms when booked and as required;

4.7.7 supervise students in ICT rooms as required, at lunch times or after school, providing technical help as necessary.

4.7.8 contribute to proposals regarding ICT equipment and software upgrades via the Network Manager;

4.7.9 carry out website maintenance including revision of site content, structure and design, in consultation with the Network Manager;

4.7.10 monitor use of ICT relating to the abuse of e-mail and the internet and misuse of ICT facilities and other acts against the Acceptable Use Guidance.

4.8 Students

4.8.1 are required to agree to the 'ICT: Student acceptable computer usage agreement' (Appendix 2) in order to continue to access the ICT system.

4.8.2 are expected to use the computer system responsibly in line with the 'ICT Acceptable Use Guidance – Students' (Appendix 2);

4.8.3 are expected to follow the simple protocol of leaving their work area tidy, when leaving the computer room; not eating or drinking in the computer rooms; and storing bags and coats safely;

4.8.4 are expected to give up their machine if they are not using it for work and someone requiring access for the purpose of work needs it;

4.8.5 report instances of misuse or malfunctioning equipment to the nearest member of staff.

4.9 Parents

4.9.1 are asked to reinforce the school's policy and practice with respect to ICT acceptable use and the dangers of inappropriate or careless use of the Internet.

4.9.2 are asked to read through the 'ICT Acceptable Use Guidance – Students' (Appendix 2) with their sons/daughters on entry to the school.

4.9.3 are informed of Oldfield School ICT acceptable use initially via the 'ICT Acceptable Use Guidance – Students' (Appendix 2) and then will receive updates via Outlook, the website and other methods as appropriate.

5 ICT Provision

5.1 The Curriculum Network

5.1.1 Except for exceptional circumstances class sizes in dedicated ICT lessons are such that each student has her/his own computer.

5.1.2 The school-wide computer network is maintained, upgraded and extended as finances permit, utilising a common set of business applications, with individual departmental requirements satisfied as appropriate.

5.2 Communications

5.2.1 The curriculum network is able to offer access to the Internet and electronic mail at any point on it to allow access via broadband connection. Students are able to research and collect data for any subject via the Internet and communicate with other students world-wide (some in foreign languages). This could enhance the teaching of any subject and will enable higher achievement in any ICT related qualification.

5.2.2 Each student is issued with their own individual electronic mail address, subject to their agreement to abide by the school's 'ICT Acceptable Use Guidance – Students' (Appendix 10). Staff and students are encouraged to make use of this for the mutual sending of legitimate education related messages, or for the submission of work.

5.2.3 The Internet Service Provider used must operate a viable filtering policy.

5.2.4 Students and, in the cases of Years 7 to 11, their parents, are required to agree to an appropriate Acceptable Use Guidance with respect to the Internet and communications.

5.2.5 An internal network-wide Intranet is maintained with frequently used websites and other relevant information, as designated by faculties.

5.2.6 The Oldfield website is developed and maintained to foster a positive external impression of the school.

5.2.7 Links between the school and the 'community' including primary liaison, industrial links and the community at large are encouraged via the Internet.

5.3 Cross Curricular ICT

5.3.1 All students in all years are entitled to use ICT to enhance and enrich their learning in all of their subjects.

5.3.2 All subject areas ensure that suitable ICT based resources and/or activities are available to enhance the learning opportunities of all students taking their subject. Activities make use of the students' available skills and ensure that good use is made of the equipment available, i.e. the computers are used as problem solving tools, a learning resource or a tool to present information/data to a high standard. Deliberate copying and pasting of information directly from an electronic source is specifically discouraged, unless required by a legitimate educational activity, in which case, the source must be acknowledged.

5.4 The Administration Network

5.4.1 Administrative staff are expected to receive appropriate training to ensure that the Administration Network is used effectively and efficiently;

5.4.2 The location of Administration Network machines are spread around the school sufficiently, to enable school-wide access to records; to enable more efficient management; and to allow teaching staff more convenient access to computing facilities.

6 Social Media

6.1 Use of social media within school

Staff are not permitted to access social media websites from the school's computers or other school device at any time unless authorised to do so by a member of the SLT. However, staff may use their own devices to access social media websites while they are in school, outside of directed times. Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute.
- Breach confidentiality.
- Breach copyrights of any kind.
- Bully, harass or be discriminatory in any way.
- Be defamatory or derogatory.

6.2 Use of social media outside of school

The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff or students by name, position or year group. Opinions offered should not bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

6.3 General considerations

When using social media staff and others should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal e-mail addresses to students or parents.
- Restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and students both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties e.g. for 'cyber-bullying' or identity theft.

Staff should not make ‘friends’ of students at the school because this could potentially be construed as ‘grooming’, nor should they accept invitations to become a ‘friend’ of any students.

Staff should also carefully consider contact with a student’s family members because this may give rise to concerns over objectivity and/or impartiality.

Staff should keep any communications with students transparent and professional and should only use the school’s systems for communications.

If there is any doubt about whether communication between a student/parent and member of staff is acceptable and appropriate a member of the SLT should be informed so that they can decide how to deal with the situation.

Before joining the school new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

6.4 Misuse of social media

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal.

6.5 Disciplinary action

Any breach of this policy may lead to disciplinary action under the school’s disciplinary policy. Serious breaches of this policy, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Students, staff and volunteers must be aware of what is considered to be ‘criminal’ when using social media/Facebook or the internet and electronic communication in general.

While the list below is not exhaustive, it provides some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

All incident types below could be considered criminal in nature but incidents would be subject to a full investigation in order to determine whether a crime has been committed or not**.**

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source, when submitting work as that of the student, e.g. in coursework or controlled assessments.
- Misuse of logins (using someone else’s login).
- Distributing, printing or viewing information on the following:
  - Soft-core pornography.
  - Hate material.
  - Drugs.
  - Weapons.
  - Violence.
  - Racism.
- Distributing viruses.
- Hacking sites.
- Gambling.
- Accessing age restricted material.
- Bullying of anyone.
- Viewing, production, distribution and possession of indecent images of children.
- Grooming and harassment of a child or young person.
- Viewing, production, distribution and possession of extreme pornographic images.
- Buying or selling stolen goods.
- Inciting religious hatred and acts of terrorism.

- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above).

6.6 Responding to misuse/incidents

Facebook (for incidents of cyber-bullying or inappropriate behaviour)

- If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed.
- Failing that, having kept a copy of the page or message in question, delete the content and take action as appropriate.
- For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
- For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column.
  - Always try to cite which of the Facebook terms and conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or community standards at http://www.facebook.com/communitystandards/.
  - Note that Facebook are more alert to US law than UK. The process should be anonymous.
- If the page is authored by someone under 13 then click on the following link: http://www.facebook.com/help/contact.php?show_form=underage .
- To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
- To report abuse or harassment, e-mail abuse@facebook.com. Facebook will acknowledge receipt of your e-mail and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint.
- If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/ .
- If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be undertaken via https://ssl.facebook.com/help/contact.php?show_form=delete_account.
- They should be made aware of the privacy issues that might have given rise to their problem in the first place:
  - You will not bully, intimidate, or harass any user.
  - You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
  - You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.

The school policies and protocols on child protection, safeguarding and e-safety must be followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will always be responded to.
- In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. If appropriate, disciplinary action will result. However, where necessary, the police will be involved and/or legal action pursued. The current Criminal Prosecution Service (CPS) guidance 'Guidelines on prosecuting cases involving communications sent via social media' came into effect on 20 June 2013 and set out the approach that prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of a communication via social media. These guidelines are helpful when used alongside school employment and disciplinary policies in cases where staff misuse may the issue.

7 Staff E-mail

7.1 Use of e-mail

The use of e-mail within Oldfield School is an essential means of communication for both staff and students. In the context of school, e-mails should *not* be considered private and staff should assume that anything they write or e-mail could become public. Therefore they should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Educationally, e-mail can offer significant benefits including direct written contact between schools on different projects, be they staff-based or student-based, within school or in an international context.

We recognise that staff and students need to understand how to style an e-mail in relation to good network etiquette (netiquette).

If data is to be sent with an e-mail then reference must be made to the Information Security Policy.

7.2 Managing e-mails

The school gives all staff their own e-mail account as a work-based tool. This school e-mail account should be the account that is used for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal contact information being revealed.

For the safety and security of users and recipients, all mail is filtered and logged. If necessary, e-mail histories can be traced.

The following rules will apply:

- Under no circumstances should staff contact students, parents or conduct any school business using any personal e-mail addresses.
- It is the responsibility of each account holder to keep their passwords secure.
- All external e-mails, including those to parents, should be constructed in the same way as a formal letter written on school headed paper (i.e. use of Dear Mr/Mrs/Ms and 'Yours sincerely', etc.).
- If any issues /complaints are involved then staff sending e-mails to parents, external organisations, or students are advised to cc their line manager.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, clarifying that any views expressed are not necessarily those of the school – see Section 5.7 below.
- ICT Technicians will set up all school staff e-mail accounts so that the disclaimer is added to all e-mails.
- All e-mails should be written and checked carefully before sending.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Staff are expected to manage their staff e-mail account in an effective way as follows:
    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
    - However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school ICT, e-safety and e-mail policies apply.
    - The use of Hotmail, BT Internet, AOL or any other internet-based webmail service for sending, reading or receiving any school business related e-mail is not permitted.
    - Staff must immediately inform their line manager/ICT Technicians if they receive an offensive e-mail.

7.3 Sending e-mails

The following rules apply:

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, please see the section below 'E-mailing personal, sensitive, confidential or classified information'.
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising (e.g. advertising/promoting a personal business, either your own or others).

7.4 Receiving e-mails

The following rules apply:

- Check your e-mail regularly.
- If appropriate, activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source. If unsure, always consult the ICT Technicians first.
- Do not use the e-mail systems to store attachments. Detach and save business-related work to the appropriate shared drive/folder.
- The setting to automatically forward and/or delete of e-mails is not allowed. Individuals are required to 'manage' their accounts.

7.5 E-mailing personal, sensitive, confidential or classified information

Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing confidential data is not recommended and should be avoided wherever possible. Staff should ensure that they have read and are aware of the Information Security Policy. The use of Hotmail, BT Internet, AOL or any other internet-based webmail service for sending school-related e-mails containing sensitive information is not permitted.

Where the conclusion is that your school e-mail must be used to transmit such data, then exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor, if unknown, before responding to e-mail requests for information.
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify.
- Send the information as an encrypted document attached to an e-mail.
  - Provide the encryption key or password by a separate contact with the recipient(s) – preferably by telephone.
  - Do not identify such information in the subject line of any e-mail.
  - Request confirmation of safe receipt.
- When sending an e-mail containing personal or sensitive data, the name of the individual is not to be included in the subject line and the document containing the information must be encrypted.
- To provide additional security you need to put 'CONFIDENTIAL' in the subject line and as a header in the e-mail and any attachments to the e-mail.

7.6 Students and e-mail

Students are introduced to e-mail as part of the ICT scheme of work. Staff should make students aware of the following when using e-mail:

- All student e-mail users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language.
- Students should not reveal any personal details about themselves or others in e-mail communication.
- Students should not use e-mail to arrange to meet anyone without specific permission.
- Students must ensure that any e-mail attachments they receive are checked for viruses before opening.
- Students must immediately inform a teacher/trusted adult if they receive an offensive e-mail.
- The forwarding of chain letters is not permitted in school. Students should forward any chain letters causing them anxiety to the ICT Technicians..
- Staff should inform other relevant staff if they become aware of any student misuse of e-mails.

7.7 E-mail disclaimer text

****

Please consider the environment before printing this email.

This e-mail and any attachments is intended to be read by the above named recipients only and the contents may be confidential, personal and/or privileged. It is for the exclusive use of the intended recipients. Therefore if you are not the intended recipient(s), please note that any distribution, forwarding, copying or use of this communication or the information in it is strictly prohibited. If you have received it in error, please contact the sender immediately by return e-mail. Please then delete the e-mail and any copies of it and do not use or disclose its contents to any person. Any personal views or opinions expressed in this e-mail are those of the individual sender and Oldfield School does not endorse or accept responsibility for them. No contractual arrangement is intended to arise from this communication. Prior to taking any action based upon this e-mail message, you should seek appropriate confirmation of its authenticity.

If you have any complaints about the content of this message please reply to:

Oldfield School
Kelston Road
Bath
BA1 9AB

Tel: 01225 423582
Fax: 01225 464986
Main School email: enquiries@oldfieldschool.com

8 Reviewing Whole School ICT

8.1 The following, where appropriate are to be reviewed at the times stated:

- resourcing requirements, at the beginning of Term 5;
- the responsibilities of Headteacher, Business Development and Finance Director, Network Manager, Head of ICT and Computing, Heads of Faculty, Curriculum Co-ordinators, staff in charge of subjects, teachers and ICT Technicians, at the beginning of the Term 5.

9 Health & Safety Issues

9.1 When taking classes to the ICT rooms, staff are asked to ensure that their classes observe the following protocol and health and safety guidance:

1. DO:

a) Line up outside the ICT room quietly. (S)
b) Listen carefully to what your teacher tells you. (S)
c) Put your coats on the back of your chair or in the racks/baskets provided. (L, H, D)

d) Put your bags on the floor (ensuring no aisle is blocked), or in the racks/baskets provided. (L, H, D)

e) Sit comfortably and look away from the screen regularly. (S)

2. DO NOT:

a) Enter an ICT room without a teacher present. (S)

b) Touch any computer equipment or log on unless told to do so. (D, S)

c) Put coats or bags on the table. (L, H, D)

d) Eat or drink in the ICT room. (L, D)

e) Spray aerosols in the ICT room. (D)

f) Move from your chair without permission. (S)

g) Tip your chairs. (D, S)

h) Play with any wires, cables or plug sockets. (E, D)

i) Touch computers with electrical faults. (S)

j) Draw on or remove labels from computers. (D)

k) Print out work unless permission has been given. (W)

HAZARDS:

L	Liquid	**H**	Heat	**E**	Electrical
D	Damage	**S**	Safety	**W**	Waste

9.2 Students using ICT rooms outside of lesson times, or using computers in any other room in the school, must comply with the above guidance with respect to behaviour and computer use in the room, in addition to any other procedures required locally in these rooms.

9.3 All projectors if misused have the potential to cause eye injury, therefore when using data projectors alone or with interactive whiteboards, the following guidance should be observed:

- Do NOT stare directly into the beam.
- When entering the beam DO NOT look towards the audience for more than a few seconds.
- Try and keep your back to the projector beam when standing in the beam.
- Supervise students at all times during the operation of the projector.

10 Computer Equipment Issued to Staff

Computer equipment, such as laptop computers, may be issued for staff use out of school either on a temporary or a permanent basis.

10.1 Permanent Loan

Before a loan can take place, the relevant loan form available from the Business Development and Finance Director must be completed, detailing the equipment description and serial number. This document must be signed by the Headteacher and the staff member borrowing the equipment. A copy of the agreement will be kept by the Headteacher, the staff member, and the Business Development and Finance Director. The latter is responsible for the loan transaction and the retrieval of the item at the end of the loan period.

The loan period will terminate under the following circumstances:

- The staff member leaves the employ of Oldfield School.
- Any breach of the loan conditions applicable on the relevant loan document.
- The staff member chooses to return the item.

10.2 Temporary Loan

Before a loan can take place, the relevant loan form (available from the staff member normally responsible for the equipment, or the Bursar or Business Development and Finance Director) must be completed, detailing the equipment description and serial number. This document must be signed by the staff member normally responsible for the equipment, the Bursar and the staff member borrowing the equipment. A copy of the agreement will be kept by the staff member normally responsible for the equipment and the staff member borrowing the equipment. The former is responsible for the loan transaction and the retrieval of the item at the end of the loan period.

11 Monitoring and reviewing

The school will monitor the impact of the policy using a range of methods and information including:

- Logs of reported incidents.
- Monitoring logs of internet activity.
- Internal monitoring data for network activity.
- Surveys/questionnaires of students, parents/carers and staff.

The policy will be reviewed in the light of any incidents that have taken place or significant new developments in the use of the technologies which may require a change to the policy, or perceived new threats related to ICT.

The policy is planned to be reviewed every two years by SLT, with the exception of the ICT Acceptable Use Guidance Appendices, which will be reviewed annually to check they remain valid and current.

Appendix 1 - Relevant Legislation

The following sections outline features of UK legislation that are applicable to the use of ICT contextualised as applicable to use within the school or used as an employee or student of the school. It is essential that the terms of this legislation are not breeched, as that would constitute an offence under the law. In addition, it is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Counter-Terrorism and Security Act 2015

Section 26 of the Counter-Terrorism and Security Act 2015 defines the schools duty to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

We approach this by providing a safe online environment. The School has internet filtering in place to block student access to violent or otherwise inappropriate materials. Students are required to accept an ICT Acceptable Use Policy when logging onto the school network. Internet usage is monitored on a daily basis and pastoral and/or disciplinary responses may follow if a student's usage breaches our rules or raises concerns. The School will also seek to block specific sites and search terms too if they appear to pose a risk to our students. Students receive advice and instruction from teaching and pastoral staff on safe internet usage.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individuals' data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this Act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes works, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:-

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the World) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically teachers, social workers, health professionals, careers advisors fall into this category of trust). Any person engaging in sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix 2 - ICT Acceptable Use Guidance - Students

Introduction
This policy is in place for the use of the Oldfield School ICT facilities by students. There is a separate policy for use by staff.

There are many computers available for use by students and the majority of these have access to the internet through the school network. All students have a login name, password and an e-mail account. The e-mail system is available for use both from within the school and externally using a web browser.
The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Students can only access data to which they have right of access.
- No student should be able to access another’s files without permission.
- Access to personal data is securely controlled in line with the school’s personal data policy.
- Logs are maintained of access by students and of their actions while users of the system.

The internet provides children and young people with a wealth of opportunities for their entertainment, communication and education. But there are also risks of harm through the deliberate behaviour of others online, and through exposure to inappropriate content. Oldfield School has procedures in place to safeguard all learners from unlawful, sexual or otherwise potentially harmful content on the internet. Information on internet safety and the importance of monitoring internet use at home is made available to all parents annually via the school website.

Objectives and Targets
The objective of this policy is to develop an appropriate code of practice for the use of ICT by students at Oldfield School.

The following code of practice must be adhered to by all students and you are expected to agree to the ICT: Student acceptable computer usage agreement (see below).

Rights of Access – Students
A safe and secure username/password system is essential and applies to all school ICT systems, including e-mail.

All passwords are generated by the ICT Technicians and are unique to each student. Passwords can only be reset by the user or by the ICT Technicians and members of the ICT teaching staff. All students have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the ICT Technicians and these are regularly reviewed. The ‘master/administrator’ passwords for the school ICT system used by the ICT Technicians are also available to the Headteacher and the Business Development and Finance Director and kept in a secure place (school safe). In the event of a serious security incident, the police may request, and will be allowed access to, passwords.

ICT Code of Practice – Students

The facilities are provided to support and enhance curriculum-related activities. Each student is issued with his/her own username and password, which must be kept confidential. Students must remember to log off when they have finished using the computer. It is good practice to change passwords regularly.

- The student's school e-mail address must always be used for all school-related activity. Personal e-mails must not be used for any school-based activity.
- The use of another person's user name and password, abusive language, sending abusive messages and changing computer settings are all serious offences.
- Students must not copy, alter, print or change another student's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.
- Students must use the internet and printing facilities only to support their school work.
- Students should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the content.

E-mails are not confidential and do go astray. Therefore we must guard against any abuse which will bring the school into disrepute.

- Students must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone unless this is part of a school project approved by their teacher.
- Students must never pretend to be anything or anyone that they are not and must be aware that the posting of anonymous messages is forbidden.
- Students must not engage with internet chatrooms.
- If a student sees something which makes her/him feel worried or uncomfortable, she/he should report it immediately to a member of staff and never respond to bullying, suggestive or unpleasant e-mails or blog entries.
- Students must not send abusive e-mail, chain e-mail, excessive quantities or excessive sized e-mails. Nor must they use e-mail to send or encourage material that is pornographic, illegal, offensive or invades another's privacy.

Students must not vandalise the system by:

- Physical damage.
- Changing configuration or cabling unless specifically directed by a member of staff.
- Hacking of the school or external systems.
- Changing the contents of the hard disks.
- Downloading or installing software onto the network, unless written as part of an approved school computer project and with the teacher's permission.
- Bringing food and drink into computer areas or in the vicinity of classroom computers because spillages can cause serious damage to electronic equipment.

Serious offences and other inappropriate use of ICT facilities will result in the following sanctions:

- An immediate ban from the network pending investigation.
- A letter home informing parents of incorrect ICT use and a minimum ban of two weeks from the internet/e-mail facilities.
- Subsequent offences will lead to a four to eight week ban and/or an exclusion of up to three days from school.
- More serious or long term abuse will lead to a total network ban and possible exclusion from school.

Misuse of Computer Systems by Students

Internet and E-mail

Please note that in the case of misuse of internet and e-mail facilities the following action will be taken:

- **First Offence** – the student will be reported to the Business Development and Finance Director/ICT Technicians and will have access to the internet and e-mail withdrawn for two weeks. The student will still have access to intranet and basic application software.
- **Second Offence** – procedure as above but with a four week ban and a letter sent home from the Head of House.
- **Third Offence** – the student will receive an internal exclusion or a fixed term exclusion, depending on the offence.

Students who use other students' accounts and access restricted file areas

These are considered to be serious offences. The ICT Technicians will record the offence and will immediately inform the Head of House of the situation. Suspension of a student's access to all ICT facilities will take place after the Head of House has informed the appropriate staff.

The length of the ban may vary according to circumstances but it is likely to be for at least four weeks.
To restore access, a note is required from the Head of House.

Damage to Hardware

If a student damages hardware, the ICT Technician will contact the Head of House. A letter will be sent to parents and the student will be charged for the damage.

Students who cause bullying whilst using the Internet/email/social networking sites

Incidents of bullying are considered to be serious offences. The ICT Technicians will record the offence and will immediately inform the Head of House of the situation. The Head of House will investigate the incident and a sanction will be issued; this could be in the form of an internal exclusion or fixed term exclusion, depending on the offence. Suspension of the student's access to all ICT facilities will take place after the Head of House has informed the appropriate staff. The length of the ban may vary according to circumstances but it is likely to be for at least four weeks. The Head of House will provide a note to restore access.

Under exceptional circumstances, such as abuse which may be detrimental to the school network, the ICT Technicians may disable a student's account with immediate effect.

ICT: Student acceptable computer usage agreement

Guidelines for all users of the school network

ICT Acceptable Use Policy – Students

As a student of Oldfield School you are entitled to use the ICT facilities and are expected to use them in a responsible way. It is the school's policy to monitor the activities of computer users on a random basis. Any complaint relating to the use of the ICT facilities will be investigated. Note that school staff may inspect the content of any file including e-mail messages at any time. If you have any queries relating to this code of conduct, please contact Mr Morris (Network Manager) or an ICT Technician.

Usernames and Passwords

- Never use a username or password allocated to another person.
- Never tell anyone else your username and/or password. You may be held responsible for anything they do in your name.
- Choose a password that you are likely to remember, but that others will not easily guess.

- Passwords may be changed and you are encouraged to do so regularly to prevent breaches of security.
- If you forget your password, your ICT Teacher or an ICT Technician will be able to give you a new one.

Responsible Use

- School ICT facilities are provided for use by students in the course of their education. Other use is generally not permitted.
- You must not pretend to be anyone else whilst sending e-mail, posting to user groups or when making information available online (for example on the Internet).
- Always use your e-mail address to identify yourself when sending e-mail.
- Never tell your address, telephone number or any other personal information to people you do not know.
- Do not post offensive information on any website about any person or organisation, or send e-mails or text messages that may be considered rude, offensive or threatening. These actions are known as Cyber Bullying and if detected will be dealt with as a serious behaviour issue.
- Do not attempt to access websites that have been blocked. These will generally include all chat rooms, social sites such as Facebook, bulletin board services, web-based e-mail, torrent sites and sites containing offensive material.
- Game playing is not permitted except for educational games used in lessons under the supervision of teachers.

Good Working Practice and Avoiding Damage to Equipment

- You must not eat, drink or place food or drink near the computers. A tiny spill or a few crumbs can easily ruin the function of delicate and expensive equipment.
- You may adjust the position of the keyboard and mouse to suit your needs, but you should not attempt to move the computer or monitor units.
- Any deliberate damage to equipment (including computers, mouse mats and furniture) will be treated as a serious breach of regulations and will be charged for.
- Computer rooms should be left in a tidy state. Remove your scrap papers, tidy away headphones if used and push your chair under the table.
- You should log off (not shut down) when you have finished using the computer.
- Computers not in the main computer rooms should be shut down at the end of the day.
- You may go to a computer room to work during lesson time, providing you have your Contact Book with you and that it has been signed in the relevant place by your teacher, that there is enough space for you in the computer room, and that if a lesson is going on, the teacher in the room agrees to your presence.
- The computer rooms (004, 005, 006, 007 and P11) are bookable for classes. If you are working in a computer room and a class arrives for whom the teacher has booked the room, you must give up your computer and leave the room if asked by the teacher.
- Report technical faults to an ICT technician. Do not attempt fixes yourself.
- Adjust your seat to obtain a comfortable working position. Avoid staring at the screen for long periods – look away from the screen occasionally to avoid eyestrain.
- Downloading and installation of large files slows the system and is not permitted, e.g. screen savers, MP3 files, games, etc.

Printing

- Remember that once you press ‘Print’, your work will be held on a print queue until you release the job on any MFD (Multi-Functional Device) located throughout the school. Jobs not released from the queue will automatically be deleted after 24 hours.

- When printing from the Internet, ‘Print’ will print the whole of the web-page you are on. This may run to lots of pages of paper, which wastes time, toner and paper. It is better to copy and paste the section you want to a new Word document, and then print that. Ask an ICT Technician or teacher for help if you need it.
- Each student is allocated a number of printer credits per term. Printing in mono costs 1 credit per page, colour 2 credits per page. You can check your current credit status by viewing the Papercut status box in the top right of your screen.

Online Information

There is a wealth of educational material online. There is also a mass of undesirable material. School policy is to log all Internet activity on the school’s ICT system. All information that you access or make available online must be considered to be legal and decent by the school. It must not be obscene, blasphemous, libellous, seditious, and racist or in any way break any UK law related to published material.

Penalties - Withdrawal of Facilities

Any student found to be in breach of this Code of Conduct may have their use of facilities withdrawn or restricted, for example loss of Internet access for a fixed period of time. In addition, students may be charged for replacements and extra work arising as a result of computer misuse for which they are directly responsible.

Breaches of the Law

Students must not publish or copy copyrighted material without permission, or claim it as their own work. In the case of serious computer misuse, where breaches of the law are found to have occurred, the police will be notified.

Appendix 3 - ICT Acceptable Use Guidance – Staff

Introduction

This policy is in place for use of the Oldfield School ICT facilities by staff. There is a separate policy for use by students.

There is a small network of computers which are used in the administration of the school (finances, student records, timetables, registers etc). Many more computers are available for use by students and staff and the majority of these have access to the internet through the school network. All students and staff have a login name, password and an e-mail account. The e-mail system is available for use both from within the school and externally using a web browser.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another’s files without permission (or as allowed for monitoring purposes within the school’s policies).
- Access to personal data is securely controlled in line with the school’s Data Protection and Information Security Policy.
- Logs are maintained of access by users and of their actions while users of the system.

Objectives and Targets

The objective of this policy is to develop an appropriate code of practice for use of ICT by staff at Oldfield School.

The following code of practice must be adhered to by staff. All staff will be expected to agree to the ICT: Staff acceptable usage agreement (see below). Staff who receive a laptop which is the property of the school will also be expected to follow the procedures outlined in Section 8 of the ICT Policy.

Rights of Access - Staff

A safe and secure username/password system is essential and will apply to all school ICT systems, including e-mail, etc.

All passwords are generated by the ICT Technicians and are unique to each member of staff. Passwords can only be reset by the user or by the ICT Technicians. All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the ICT Technicians and these are reviewed regularly. The "master/administrator" passwords for the school ICT system used by the ICT Technicians are also available to the Headteacher and the Business Development and Finance Director and kept in a secure place (school safe). In the event of a serious security incident the police may request, and will be allowed access to, passwords.

Staff are reminded to never leave their computer unattended when it is logged on to their user account, to prevent unauthorised access to data. Always either lock the keyboard and screen or log off.

E-mails

The computer resources at Oldfield School belong to the school and are to be used solely for educational or business purposes, although the governors will permit limited use for personal purposes, provided that it does not interfere with work performance and provided that rules of usage are observed.

E-mail is an essential tool at the school and all members of staff must read and abide by the guidance on use of e-mail in Section 5 of the ICT Policy when managing their e-mail accounts, sending e-mails, receiving e-mails and especially if e-mailing personal, sensitive, confidential or classified information.

Internet and Intranet

The internet is not necessarily secure and school sensitive information could be viewed by unauthorised individuals.

- Staff must abide by the current restrictions on correspondence or the passing of information to outside organisations or individuals.
- The transmission of school sensitive data over the internet is strictly prohibited.
- At no time may staff use the internet to send school or personal information that would, if intercepted, place the school in violation of UK laws or regulations.
- Staff may not use the internet to view illegal, pornographic or seditious material that would place the school at legal risk.
- Staff may not download or distribute material from the internet without virus checking. Users are responsible for virus checking any material.
- Staff must not gain unauthorised access to the internet e.g. by hacking or by trying to circumvent any 'blocking' controls.
- Staff must not use another individual's user identity to access the internet or intranet.
- Staff may not download screensavers, or excessive sounds, images, or audio-visual materials for storage on local PCs, or the network.
- Staff may not use the internet for private business purposes or private commercial gain.
- The ordering/purchasing of goods over the internet is subject to the same authorisation procedures and limits as purchases made by other means and failure to follow the correct procedure may result in disciplinary action.
- Staff must not engage inappropriately with students through social networking sites. Staff must be mindful that all postings on social network sites are widely accessible. See also the social media policy.

Note. There have been many instances reported of electronic communication systems, and their output, challenging the professionalism of school staff. Colleagues should be guarded in their use of all such systems.

Laptop Computers and Other Devices
Laptops, ipads, tablets and similar devices which are the property of the school fall under the same restrictions of use as networked computers. Serious misuse of laptops will be treated as a disciplinary offence and may result in dismissal. Loss, damage or theft of a laptop through misuse, or negligence may result in financial sanctions.

Laptops and peripherals should be kept in a secure place and transported in the car boot. When not in use, the laptop should be switched off and kept in its case.

Misuse of Computer Systems by Staff
Misuse or abuse of computer systems by staff is a serious matter and will be dealt with under the school's disciplinary procedures. The penalties for improper use may include dismissal, either with, or without notice. The following are expressly prohibited:

- The unauthorised export or transmission of school software via the internet.
- The accessing, viewing, downloading or forwarding of pornographic material or material of a racist or inflammatory nature.
- The loading, downloading or forwarding of games software.
- The generation or forwarding of 'chain' messages or letters.
- The sending or forwarding of abusive or offensive e-mails – inside or outside the school – or material that could cause offence. This applies to all e-mail, whether intended for person-to-person communication or wider distribution.

The list may be added to at any time. Known pornographic sites on the internet will be blocked and filters to intercept prohibited material and offensive language are in place. The school reserves the right to intercept, monitor, analyse and read all e-mail generated, received or distributed via the school networks, equipment and e-mail addresses.

Some e-mail systems have the capability to send the contents of messages to fax machines. This policy applies equally to such messages and documents.

Any queries regarding this policy should be addressed to the Headteacher or the Business Development and Finance Director.

ICT: Staff acceptable computer usage agreement

- I will only access the system with my own name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.
- If I have reason to believe my password is no longer secure I will change it immediately. I will inform the ICT Technicians as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- I acknowledge that the computer/laptop provided for me to use (if appropriate) remains the property of the school and should only be used for school business.
- I will not access the files of others or attempt to alter the computer settings.
- I will not update web logs or use pictures or text that can identify the school without the permission of the Headteacher.
- I will not alter, attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- I will follow the guidance provided by the ICT Technicians to ensure the anti-virus protection on my laptop is kept up-to-date.

- I will check with the ICT Technicians should I need to install additional software.
- I will always adhere to the school's ICT related policies
- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I understand that the school may monitor the internet sites I visit.
- I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
- I understand that staff are not permitted to access social media websites from the school's computers, staff laptop or other school device at any time unless authorised to do so by a member of the SLT.
- I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the ICT Technicians/Headteacher/ Business Development and Finance Director as appropriate.
- Any e-mail messages I send will not damage the reputation of the school. All joke e-mails and attachments are potentially damaging and undesirable and therefore will not be used.
- I will report immediately to the Headteacher any unpleasant material or messages sent to me.
- I will not post anonymous messages or forward chain letters.
- I understand that use of the school's equipment for personal financial gain, gambling, political purposes or advertising is forbidden.
- I understand that storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- I understand that I am responsible for the safety of sensitive school data that I use or access.
- In order to maintain the security of data I will take the following steps:
    - I will store data files in my user area only for as long as is necessary for me to carry out my professional duties.
    - I will not save data files to a PC or laptop other than that provided by the school.
    - I will not share or give out any passwords that I use to access school systems. If I have reason to believe that my password is no longer secure I will change it.
    - I will not use e-mail to transfer data files but save them to the school network area if other staff need access to the information.
    - If I am in any doubt as to the sensitivity of data I am using I will refer to the school's Data Protection and Information Security Policy to check. Sensitive data could include:
        - Student reports.
        - SEN records.
        - Letters to parents.
        - Class-based assessments.
        - Exam results.
        - Whole school data.
        - Medical information.
        - Information relating to staff e.g. performance reviews.

I understand that if I do not adhere to these rules outlined in this agreement, my network access could be suspended, my laptop removed and that other disciplinary consequences may follow, including notification to professional bodies, where appropriate.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.