BOLTON SCHOOL

ICT and General Data Protection Regulation Policies

Written by:	T Fox, Head of ICT
Date published:	05/04/16
Approved by:	Senior Officers
Date Approved:	25/04/16
Last Reviewed by:	Clerk & Treasurer
Date of last Review:	September 2017
Date next Review is due:	September 2018
Manager responsible for next Review:	Clerk & Treasurer

Contents

General Policies for all Users

Pupil Policies

1. GENERAL CONDITIONS

1.1 INTRODUCTION AND SUMMARY

These policies apply to all Users of School ICT resources, whether on campus or from remote locations and form part of the conditions of employment for employees, and are part of any contractual agreements with suppliers and customers.

All ICT equipment provided by the School to any employee or other person authorized by School to use the ICT equipment is intended for their sole use and must not be made available to any third party including family members. Any use of the device or system will be deemed to be made by the individual to whom the equipment is provided. All use of the device can be recorded and monitored and any misuse will be dealt with in accordance with the School's enforcement procedures.

1.2 DEFINITIONS

Bolton School	Includes Bolton School Girls' Division, Boys' Division, Central Services, Patterdale Hall and Bolton School Services Limited (BSSL) and will be referred to throughout this document as Bolton School.
AUP	Acceptable Use Policy for Information Technology.
ICT Resources & equipment	ICT resources include, but are not limited to: desktop computers, laptops, notebooks, netbooks, tablets, iPads, portable storage devices, mobile and smart phones, computer networks, peripherals, application and electronic mail applications, memory cards, which are owned by Bolton School.
User	Any authorised person who makes any use of any Bolton School ICT resource from any location. For example, Users include those who access ICT resources in a School computer suite, or via a network.

1.3 PURPOSE OF THE ICT POLICIES

The purpose of the ICT policies is to:

- communicate the Bolton School ICT policies to all Users who have access to Bolton School's computer systems;
- ensure an Information and Communications Technology infrastructure that promotes the basic missions of the School in teaching and learning, research and administration;
- ensure the integrity, reliability, availability, and performance of ICT resources;
- ensure that use of ICT resources is consistent with the principles and values that govern use of other School facilities and services;
- ensure that ICT resources are used for their intended purposes;
- establish processes for addressing policy violations and sanctions for those committing violations;
- protect both Bolton School and all individuals who need to use Bolton School's ICT equipment to carry out their work by defining what is acceptable use.

1.4 PRINCIPLES

The principles upon which the policies are based are to:

- ensure the availability of data and processing resources;
- provide assurance for the confidentiality and integrity of the data;
- ensure the integrity of data processing operations and protect them from unauthorized use;
- ensure the confidentiality of the data, and prevent unauthorized disclosure or use;
- prevent the unauthorized and undetected modification, substitution, insertion, and deletion of that data.

1.5 SCOPE

The Bolton School ICT policies apply to all School data assets that exist in any School system or processing environment on any media during any part if its lifecycle.

The following Users are covered by the policies:

- full and part-time employees, including those on temporary or fixed term contracts;
- suppliers and contractors who have access to systems;
- pupils;
- volunteers;
- other persons who have access to the School's systems or data.

1.6 POLICY MANAGEMENT

A biennial review of the Bolton School ICT policies will be conducted by the Head of ICT Services and approved by the Senior Officers.

1.7 POLICY AVAILABILITY

The ICT policies are readily available in electronic format on the School intranet.

1.8 DISTRIBUTION TO NEW USERS

As part of the School staff recruitment and induction process, all new employees will be given copies of the policies and asked to confirm they will adhere to the principles herein through signing the ICT Acceptable Use Policies Acceptance Form.

1.9 DISTRIBUTION TO CURRENT USERS

The policies will be distributed to all currently authorized Users of the School systems. They will be regularly asked to acknowledge receipt and confirm they will adhere to the principles herein.

1.10 ENFORCEMENT

Users who violate the ICT policies may be denied access to School ICT resources and may be subject to other penalties and disciplinary action, including for employees, dismissal. Alleged violations will be handled through the School disciplinary procedures applicable to the User. The School may suspend, block or restrict access to an ICT account, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of School or other computing resources, or to protect the School from liability or reputational damage. The School may also refer suspected violations of applicable law to appropriate law enforcement agencies. Severe, deliberate or repeated breaches of the policy may be considered grounds for employee dismissal; or in the case of other Users, termination of the contractual agreement under which their use is authorized; or in the case of Pupils, other sanctions as deemed appropriate by the School. All employees and other authorized Users are bound by this policy and are responsible for its strict enforcement.

1.11 DISCLAIMER OF LIABILITY

Bolton School disclaims all liability for any damages, consequential or otherwise, costs, fines or penalties arising out of the use of any ICT equipment and systems by any User, whether or not in contravention of any clause contained within this policy.

1.12 RELEVANT LAW

The Equality Act 2010
Defamation Act 1996
Data Protection Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699
Employment Practices Data Protection Code (on Information Commissioner's website)
General Data Protection Regulation 2018

Acceptable Use of ICT Equipment and Systems Policy

2. ACCEPTABLE USE OF ICT EQUIPMENT AND SYSTEMS

All ICT equipment, systems and networks (including, but not limited to, office software, the internet, e-mail, telephone and transactions systems) are for School use. Reasonable personal use is permitted provided that this does not interfere with the performance of the School's business, or prevent other Users from performing their duties or contravene any of the ICT policies.

When using ICT systems, Users are expected to conduct themselves in a trustworthy and appropriate manner so as not to discredit or harm the reputation of Bolton School or any of its Governors, employees or pupils.

Users should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to ICT Services. Users are not permitted to interfere with or make any adjustments to any hardware settings of a School-owned ICT device, or to any other peripheral or cabling unless authorised to do so by ICT Services.

Employees and other Users are not permitted to make purchases of ICT equipment on behalf of Bolton School, including mobile devices. Procurement and installation of all Bolton School ICT equipment will be performed and managed by ICT Services.

2.1 SECURITY

Users must ensure that ICT equipment is logged out or locked away when left unattended at any time. It is prohibited to leave any ICT device displaying confidential data unattended at any time.

All ICT equipment should be security marked. If Users are aware of School-owned ICT equipment that does not have a security mark, they should inform ICT Services.

2.2 CONNECTING TO THE NETWORK

Wireless access is provided to School ICT network facilities for use by authorised Users. Access information for connecting to the wireless network is available from ICT Services.

Users are not permitted to physically connect any electronic ICT device which isn't owned by the School to the School network. The use of Pendrives is permitted for Employees but not for Pupils.

Users must not attempt to bypass network security protocols; this will be deemed a breach of security and will result in disciplinary action.

2.3 PREVENTING THE SPREAD OF MALICIOUS SOFTWARE (VIRUSES)

Bolton School uses up-to-date and sophisticated anti-virus systems to detect computer viruses and to reduce or prevent damage caused by a virus that enters Bolton Schools' network systems. This software is deployed automatically to all School-owned ICT equipment and installed, where possible, to mobile devices.

Any ICT equipment, regardless of ownership, must have up-to-date Anti-Virus scanning software operating before it can be connected to the School network via any permitted means. Notification of a virus on either a School ICT computer or device or a personal device connected to the School network, must be immediately reported to the ICT Services Helpdesk and further use of the device suspended until a member of ICT Services confirms its safe use.

Users may discuss any concerns about antivirus protection with ICT Services who will assist with the installation of suitable antivirus software.

2.4 SOFTWARE INSTALLATION AND LICENCING

All Users must follow School procedures for procuring software to ensure it is suitable and licensed for use on the School ICT network. All School software licences are managed and monitored by ICT Services.

Only approved software, or that for which the School has an evaluation licence may be installed on School systems and equipment. Approved software is defined as that procured by the official School order process through ICT Services.

Software without a valid licence will not be installed on the School ICT network (see Piracy).

2.5 PRINTING AND PHOTOCOPYING

Access to printing and photocopying facilities is provided for School business only. All Users are requested to use the School's printing facilities, particularly colour printing, sparingly and use the School photocopying facilities as the preferred means for producing School handouts and other documents. All School photocopying must be done in compliance with the School's Copyright Licensing Agency (CLA) licenses and the Copyright, Designs and Patent Act (1988).

Online systems and shared file storage areas are provided as alternative means to share documents.

2.6 MONITORING

The use of all School ICT systems is monitored. This includes but is not limited to:

- reviewing e-mails sent and received by employees and other Users;
- monitoring the web sites employees and other Users visit on the Internet;
- the length of time employees and other Users use the Internet;

- reviewing material downloaded or uploaded by employees and other Users.

For the purposes of (amongst other things):

- ensuring that the ICT system is not being misused;
- detecting or preventing crime;
- ensuring School business continuity;
- establishing facts.

Bolton School also reserves the right to keep copies of any data and/or documents regarding the use of the Internet and email, and if it sees fit, to use this information if required in legal or disciplinary proceedings.

Bolton School may bypass passwords or any other form of security set by Users. ICT Services has the authority to fully access any PC, ICT system or device belonging to Bolton School.

All communications and stored information, sent, received, created or contained within Bolton School's ICT system remains the property of Bolton School, and accordingly should not be considered private. No person using the ICT system can have an expectation that his or her use of that system is private. Such use is permitted strictly on the understanding that all Users accept this principle. However, the type of stored information will be at the User's discretion and under normal circumstances ownership should be clear. Please note this will not affect individual statutory intellectual property rights over original work. If Users are unsure of their rights of ownership, clarification should be sought from the Head of ICT.

2.7 PIRACY

Piracy is the unauthorised copying of computer software or other copyright material. It is a form of theft. Under the Copyright, Designs and Patents Act (1988), copyright infringement can lead to legal action and criminal proceedings against Bolton School and the individual concerned.

Users must inform ICT Services if they suspect that unapproved software has been installed on a Bolton School computer or other ICT device.

Users must not:

- use any unapproved software which has not been purchased via the School's official ordering process;
- distribute unauthorised software to anybody;
- make unauthorised copies of computer software.

Acceptable Use of Internet and Social Networking Policy

3. ACCEPTABLE USE OF THE INTERNET, SOCIAL MEDIA OR MESSAGING SERVICES

All internet access provided by the School is subject to the terms of this policy regardless of the device used and the method in which the device is connected.

Users must not knowingly:

- visit, view, download or upload any material from any website, social network or messaging service which, in the opinion of the School Management, contains obscene, sexist, racist, otherwise discriminatory or illegal material;
- conduct or encourage any activity that may be illegal;
- send or post Bolton School confidential data without appropriate written authorisation;
- send or post any messages that may damage Bolton School's image or reputation, or otherwise harm its interests;
- access any internet sites that may result in an unauthorised financial charge to Bolton School;
- enter into any contracts or commitments in the name of or on behalf of the School.

Any User who accesses any site on the internet, either deliberately or inadvertently, which he/she feels is inappropriate must report it to ICT Services immediately.

Where Users are permitted access to the internet at School they are expected to use it sensibly and in such a manner that it does not interfere with the efficient running of the School.

These policies also apply to Users of Bolton School ICT equipment or systems off-site. When used off site, Users are permitted to make use of alternative internet connections, providing that the internet is accessed in a controlled manner, where the necessary firewalls and virus protection are in place.

The School reserves the right to deny internet access to any User, although in such a case it will give reasons for doing so.

3.1 WEBSITE REGISTRATION

Many sites that could be useful for the School require registration. Users wishing to register as a User of a website for work purposes are permitted provided this would not result in a cost to the School and/or they have permission from the relevant budget holder.

Some websites may require the School to enter into licence or contract terms. The terms should be sent in advance for approval by the Head of ICT, before a User agrees to them on the School's behalf.

3.2 MONITORING OF INTERNET USE

All internet usage via Bolton School ICT resources is monitored. The School's Senior Officers consider the following to be valid reasons for checking a User's internet usage:

- If it is suspected that the User has actively been viewing offensive or illegal material, such as material containing racist terminology or nudity;
- If it is suspected that the User has been spending an excessive amount of time viewing websites that are not work related;
- Preventing or detecting illegal or inappropriate activity;
- Ensuring Bolton School's business continuity;
- Investigating or detecting unauthorised use of internet facilities.

In the event that the monitoring procedure indicates the possibility of misuse of the internet facility by a User, a report will be made by the Head of ICT Services to the School Senior Officers.

3.3 SOCIAL NETWORKING

The School recognises that Users may use the internet for personal purposes and may participate in social networking. In order to reduce exposure to claims of defamation in respect of materials published by Users, extreme care should be taken when making use of this type of site.

If using authorised Bolton School Social Networking accounts, all usage must be in compliance with Bolton School policies.

3.4 PERSONAL AND PRIVATE USE

Reasonable personal use of the internet is permitted provided that this does not interfere with the performance of Bolton School's business or prevent other Users from performing their business at Bolton School or contravene any relevant Bolton School policy.

Users are not permitted to access social networking websites on the internet for personal use during times when they should otherwise be conducting Bolton School business.

The School's Senior Officers reserve the right to restrict access to these websites.

Personal use of the internet is a privilege and not a right.

3.5 PERSONAL CONDUCT

Bolton School respects a User's right to have a private life outside of School business. However, in order to ensure that confidentiality and its reputation are protected, Users of social networking websites for personal and private use must:

- ensure that they do not conduct themselves in a way that is detrimental to the School;
- not publish any information that could damage the reputation of the School;

- take care not to allow their interaction on these websites to damage working relationships between other Users and the wider School community;
- refrain from joining any online “group” where issues specific to Bolton School may be discussed, except where that group is hosted on a School system.

Any comments on any social networking site about the workplace or colleagues, made by individuals who are identifiable as employees of Bolton School, will be deemed to have been made “at work” and all Bolton School workplace policies will apply.

Any comment of a discriminatory nature or which is in breach of the School Equality and Diversity Policy and Procedure will be treated as more serious if made on a social networking site.

3.6 COMMUNICATION WITH PUPILS

Employees and other Users must recognise that communication with pupils through social networking sites could compromise status and authority, but may also raise accusations of ‘grooming’.

It is inadvisable for employees and other Users to:

- communicate with pupils via social networking sites except where it has been set up by the School to enable communication with pupils;
- follow or add current pupils or pupils who have left School within the last academic year, as friends on personal social networking sites.

3.7 SECURITY AND IDENTITY THEFT

Users should be aware that social networking websites are a public forum, particularly if the User is part of a "network". Users should not assume that their entries on any website would remain private and they should never post abusive or defamatory messages.

Users must be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, Users should:

- ensure that no information is made available that could provide a person with unauthorised access to the School and/or any confidential information;
- refrain from recording any confidential information regarding the School on any social networking website.

3.8 PERSONAL WEBSITES AND BLOGS

Users are free to set up personal blogs or social networking sites on the internet, provided that they do not breach the law or disclose School secrets, breach copyright, defame the School or its suppliers, customers, pupils or employees, or disclose personal data or information about any individual that could breach the Data Protection Act (1998). They must not include material that is sexist, racist or otherwise actionable, or bring the School into disrepute.

Users are not permitted to write their personal blog in School's time. Blogs must not disclose information that is confidential or proprietary to the School or to any third party that has disclosed information to the School. They must not be used to damage Bolton School's image, reputation or business interests whether intentionally or otherwise. Users must not link their personal blogs to the School's website or internet systems.

3.9 SCHOOL BLOG SITES

Blogs set up by the School and used by its employees and pupils for the professional workings of the School should follow the same principles as in 3.8 above.

3.10 DEFAMATION / LIBEL

The Internet and email are considered to be forms of publication and accordingly fall within the scope of legislation relating to libel. Both words and pictures are capable of being libellous if they are untrue, ridicule a person/company and as a result damage that person/School's reputation. As such, Users must take care not to knowingly make any defamatory statement that is published on the internet. Should they do so they may be legally liable for any damage to the reputation of the individual concerned and furthermore, if they are an employee of the School, the School may be held vicariously liable for this act, even if performed without the consent or approval of the School. The School may take legal action against the individual responsible if a defamatory statement is made in connection with its business or trading reputation. General employment legislation and the laws of libel preclude employees from making defamatory statements about their employer or bringing it into disrepute. In practice English law gives employees freedom of speech provided that they do not breach other laws in exercising it.

3.11 COPYRIGHT, DESIGNS AND PATENTS ACT 1988

Legal action can be taken by the copyright owner against both Bolton School and the individual(s) concerned for *unauthorised* use of any copyrighted material. Before reproducing any downloaded material Users must find out who owns the copyright and seek that person's/organisation's permission before using it.

Acceptable Use of Email Policy

4. SCOPE

For the purposes of clarification in this policy, e-mail includes electronic messaging involving computers, smartphones, mobile devices and computer networks.

The policy applies to the use of any ICT facilities, including hardware, software and networks provided by the School, for the purpose of sending or receiving e-mail messages and attachments.

All e-mail sent and received by the School servers is owned by the School and will be scanned by the School e-mail filtering system, which will block unsuitable e-mails or e-mails that are deemed unacceptable in accordance with the terms of this policy.

4.1 PERSONAL AND PRIVATE USE

The School's e-mail system is primarily for business and School use. It is permissible to use the e-mail system for personal use, provided that this does not interfere with the performance of Bolton's School's business or contravene any of Bolton School's policies. Personal use of e-mail is a privilege and not a right.

4.2 CONTENT OF E-MAILS

Users are responsible for all e-mails they send and for contacts made which may result in e-mail being received. E-mail should be treated in the same way as any other form of written communication and, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an e-mail communication. Anything that is written in an e-mail is treated in the same way as any form of writing. Users should not include anything in an e-mail which is not appropriate to be published generally.

All e-mail communication, regardless of device used, must reflect the standing and policies of the School.

The use of e-mail by employees to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the School's disciplinary procedure. In serious cases this could be regarded as gross misconduct and could lead to dismissal.

If a User receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, he/she must not forward it to any other address, either internally or externally and should immediately report it to ICT Services.

Users must not cause e-mail congestion by sending unnecessary messages or by copying e-mails to others who do not need to see them. E-mails should not normally exceed a maximum size of 5MB.

4.3 INAPPROPRIATE USE OF EMAILS

Whilst not an exhaustive or comprehensive list, the following uses of e-mail are considered inappropriate and unacceptable.

In general, e-mail must not be used for the initiation or re-transmission of:

- Chain mail - E-mail sent repeatedly from User to User, with requests to send to others.
- Harassing or hate-mail – mail which is perceived by the recipient as being threatening or abusive.
- Spamming or e-mail bombing attacks - Intentional e-mail transmissions that disrupt normal e-mail service.
- Junk mail - e-mail that is not related to School business or is sent without a reasonable expectation that the recipient would welcome receiving it.
- False identification - Any actions that defraud another or misrepresent or fail to accurately identify the sender.
- Any messages that in the opinion of the School management may damage Bolton School's image, reputation or business interests.
- Bolton School confidential data without the appropriate written authority.
- Messages that solicit personal business ventures, or advertise for personal enterprise.
- Communications with destructive or malicious intent.
- Messages, files or other materials (including pictures and sounds) which are unprofessional, vulgar, profane, insulting, offensive, harassing, defamatory, deceptive, abusive, racially offensive, sexually offensive, discriminatory (on the grounds of ethnic origin, sexual orientation, religion, belief, race, sex, gender, age or disability) or which otherwise violate the rights of another.
- Messages that conduct or encourage any activity that is or may be illegal.

4.4 PREVENTING THE SPREADING OF MALICIOUS SOFTWARE

Users of School e-mail must take all reasonable steps to prevent the receipt and transmission of malicious software e.g. computer viruses.

In particular employees:

- must not transmit by e-mail any file attachments which they know to be infected with a virus;
- must ensure that an up-to-date anti-virus system is operating on any computer which they use to access School ICT facilities;
- must not open e-mail file attachments received from unsolicited or untrusted sources;
- must not initiate or re-transmit virus hoaxes.

Virus notifications should be reported in accordance with the School's Data Security policy.

All outgoing Bolton School e-mails are automatically scanned for the presence of computer viruses.

4.5 E-MAIL COMMUNICATION WITH PUPILS

All electronic communication with pupils must be via School systems and at no time must employees, volunteers, VMT's or other adults from School communicate with pupils using their own personal e-mail address.

The School is mindful that there may be times when pupils contact employees from their personal email address. The employee must assess the appropriateness of this, only responding if the communication is related to the professional workings of the School and it is considered that the pupil understands the implications of using their own personal email for such use. Any concerns regarding such correspondence should be discussed either with the appropriate Head of School or the employee's Line Manager.

When considering a response, the employee should note the pupil's email address and be aware that responding to improperly named email addresses could be considered as inappropriate and unacceptable.

4.6 MONITORING OF E-MAIL

The e-mails sent using the School e-mail system are monitored, including deleted items. The School Senior Officers consider the following to be valid reasons for checking a User's e-mail:

- If the User is absent for any reason and communications must be checked for the smooth running of the business to continue;
- Preventing or detecting illegal or inappropriate activity;
- Investigating or detecting unauthorised use of e-mail facilities;
- If it is suspected that the User has actively been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity;
- If it is suspected that the User has been using the e-mail system to send and receive an excessive number of personal communications;
- If it is suspected that the User is sending or receiving e-mails that are detrimental to the School.

When monitoring e-mails, ICT Services will, save in exceptional circumstances; confine itself to looking at the address and heading of the e-mails. ICT Services will avoid, where possible, opening e-mails clearly marked as private or personal without prior approval from the Senior Officers.
In the event that the monitoring procedure indicates the possibility of misuse of the e-mail facility, a report will be made by the Head of ICT Services to the Senior Officers.

4.7 CONFIDENTIAL INFORMATION

No e-mail transmission is totally secure. As a consequence, information of a confidential nature should not be sent via e-mail unless expressly required by the intended recipient, who must be made aware of the potential security risk before the e-mail is sent.

No confidential, personal data or sensitive information is to be communicated by external e-mail without prior authorization from either a Senior Officer or the Data Owner in accordance with the Data Security Policy.

A disclaimer is automatically attached to every external e-mail transmission confirming that the content of the e-mail is confidential and intended solely for the use of the individual or entity to which it is addressed.

4.8 E-MAIL SIGNATURE

A standard Bolton School e-mail signature template for appending to e-mails is available for those who wish to use it. Bolton School employees are strongly encouraged to use it as their default email signature to ensure consistent and professional internal and external communications. ICT Services can assist Users to make this an automatic addition to their e-mail communications.

4.9 LEGAL ISSUES

Emails will be retained for the retention periods as specified in the School's Data Protection Policy.

Bolton School may be legally obliged to disclose e-mail messages (deleted or otherwise) in civil and criminal proceedings. This includes employment tribunals.

An e-mail can constitute a contract. Users must ensure their words do not indicate a commitment they cannot keep or are not authorised to make.

4.10 DEFAMATION / LIBEL

The Internet and email are considered to be forms of publication and accordingly fall within the scope of legislation relating to libel. Both words and pictures are capable of being libellous if they are untrue, ridicule a person/company and as a result damage that person/School's reputation. As such, Users must take care not to knowingly make any defamatory statement that is published on the internet. Should they do so they may be legally liable for any damage to the reputation of the individual concerned and furthermore, if they are an employee of the School, the School may be held vicariously liable for this act, even if performed without the consent or approval of the School. The School may take legal action against the individual responsible if a defamatory statement is made in connection with its business or trading reputation. General employment legislation and the laws of libel preclude employees from making defamatory statements about their employer or bringing it into disrepute. In practice English law gives employees freedom of speech provided that they do not breach other laws in exercising it.

Acceptable Use Policy for iPads & Laptops

5. ACCEPTABLE USE POLICY FOR IPADS & LAPTOPS

The device (iPad or Laptop) remains School property and all Users will follow these procedures for its use. Please note that all appropriate existing IT Acceptable Use Policies also apply to the device. Devices will be labelled in the manner specified by the School so that they are easily identifiable. Each device will be asset tagged and recorded on the School inventory. The use of technology resources provided by Bolton School is not transferable or extendible to other people or groups not employed at the School and terminates when a member of staff no longer works at the School.

Bolton School reserves the right to investigate a device to ensure compliance with this Acceptable Use Policy.

- You are responsible for the general care of the device that has been issued by the School. Devices that are broken or fail to work properly must be taken to ICT Services for an evaluation of the equipment.
- You are expected to make reasonable efforts to avoid the theft of the portable device.
- You will be personally responsible for any content on your device and for any use of your device.
- Passwords / PIN codes / Keypad locks must be used to restrict access to your device.
- In School and at home, your device will come under the control of a Device Manager. This will govern what you can or cannot do with your device. Staff should not make any attempt to circumvent this management process.
- If technical difficulties occur, the device may be restored to its default settings. Although every effort will be made, the School does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.
- Upgrade versions of licensed software/apps are available from time to time. Staff will be required to allow the installation of software updates to their devices.
- Individual Users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the School.
- The device has a camera and video. The School policies on taking, storing and distributing images of staff and pupils apply.

5.1 DECLARATION

- I will immediately upon delivery of the device, inspect it and notify ICT services of any defect. In the absence of such notification it shall be conclusively presumed that the device is in good working order and condition.
- I will notify the ICT Office and also by email to helpdesk@boltonSchool.org.uk immediately if the device is lost, stolen or damaged. This is vital to secure the device and for any insurance arrangement to be valid. In certain circumstances, iCloud can be used to track stolen devices.
- I will not leave the device unattended in an unlocked vehicle, in the open air, in a public place or in any outbuilding, i.e. I will ensure it is kept within sight or control at all times when in these places.

- If the device is left unattended in a locked vehicle, then it will be in the locked boot of a saloon car, or concealed under the rear parcel shelf of a locked hatchback car, or concealed in the spare wheel or other closed compartment of a locked estate car.

5.2 GOOD PRACTICE IN CARE OF IPADS

- Do not remove the device from its protective case.
- Only use a clean, soft cloth to clean the screen; do not use cleansers of any type.
- The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen. Therefore, do not lean on the top of the device when it is closed. Do not place anything near the device that could put pressure on the screen. Do not place anything in the carrying case that will press against the cover.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Devices should not be used near food or drinks, which might spill on them.
- The device must not be left in a place that is experiencing extreme hot or cold conditions (eg. car in summer or winter). Extreme heat will damage the unit itself. Extreme cold will cause severe screen damage.
- Outside School, the iPad must be carried in a bag, rather than openly in your hand. If there are other belongings in the bag, these must be kept to a minimum to avoid placing too much pressure and weight on the iPad screen. Do not carry the iPad in a bag containing any liquids which might spill on to the iPad and cause damage.
- Do not disassemble any part of any device or attempt any repairs.

User agreement

I have read and understood the Bolton School Acceptable Use Policy for iPads & Laptops.

I agree to abide by the stated rules.

I accept that any infringement of these rules will result in appropriate action by the School.

Name ____

(Please print clearly)

Signature ___________________________ **Date** _________________

Acceptable Use Policy for Telephones, Smart Phones, Mobile Phones & Devices and Internet Telephony

6. PERSONAL AND PRIVATE USE

Bolton School provides its employees with access to a telephone and, if applicable, a mobile or smartphone for work-related purposes.

School mobile telephones may be used for a limited amount of personal use, provided that this does not interfere with the performance of your duties, prevent other employees from performing their duties or contravene any of the ICT policies.

Upon request, Bolton School will require employees to repay, either by deduction from salary or any method acceptable to Bolton School, the cost of personal phone calls, text messages and other personal use of a School's mobile telephone to the extent that incremental costs have been incurred by the School for such usage.

6.1 RESPONSIBILITIES OF USERS OF MOBILE PHONES

1. Users are required to take good care of the mobile phone and take all reasonable precautions to ensure that the device is not damaged, lost or stolen.

2. Users are required to keep mobile phones clean, and in serviceable condition to the best of their ability, and report all irregularities to the ICT department.

3. A PIN Code / Keypad lock should be used to lock the mobile phone so that if the phone is stolen or lost data will be unable to be retrieved from it.

4. Mobile phones must not be left unattended.

5. SIM cards should not be swapped from one mobile handset to another unless authorized by ICT.

6. If the mobile phone is no longer required it should be returned to ICT.

6.2 CALLS, TEXT AND DATA.

1. If the mobile phone is used for private use Bolton School will, upon request, require employees to repay the costs of phone calls, text messages and data to the extent that incremental costs have been incurred by the School for such usage.

2. If the mobile phone is to be taken out of the country Users must inform the ICT department so that they can setup the correct roaming tariff for the number.

3. If Users are not connected to wireless and their phone supports email they should change the settings so it will only retrieve data when asked.

4. If available Users should connect the mobile phone to wireless to prevent data charges.

It is not permitted to use School telephones to:

- carry out freelance work, or work for another employer;
- buy or sell goods, other than when authorised to do so in the course of their job;
- gamble;
- communicate information that is confidential to the School outside the School, unless authorised to do so by either one of the School's Senior Officers or the Data Owner, as appropriate;
- chat for lengthy periods of time to friends, relatives or other persons if not conducting Bolton School business;
- make overseas telephone calls other than when required to do so for Bolton School business;
- access inappropriate content on the internet (see acceptable use of internet and social media);
- view, access, download, upload or produce any content which contravenes the School policy for use of internet and social media; this includes but is not limited to content that is sexist, racist, pornographic or discriminatory;
- take inappropriate photographs or videos either for storage or onward communication.

6.3 APPROPRIATE USE OF MOBILE TELEPHONES

School mobile telephones are provided at the discretion of Bolton School on the basis of business need, and must be returned upon request and always before the last day of a User's employment.

The safeguarding of School mobile telephones is the User's responsibility. They should not be left in a visible place such as in an unattended car. If the phone provides open access to School data and communication systems, the security of the data must comply with the School Data Security Policy.

Loss of a School mobile telephone should immediately be reported to the Head of ICT Services.

6.4 MONITORING

The School monitors usage of all School telephones for security reasons and to deter/detect unauthorised use.

Monitoring consists of random checks on the telephone numbers dialled, the websites accessed, messages received and sent, any apps (programs) used and any data stored on the device. Spot checks may also be carried out. The results of any monitoring will be maintained in strict confidence and disclosed only to Senior Officers if this is deemed appropriate.

6.5 LEGAL ISSUES

Since 1 December 2003, under the Road Vehicles (Construction and Use) Regulations 1986, as amended by the Road Vehicles (Construction and Use) (Amendment) (No.4) Regulations 2003, it has been an offence to use a hand-held mobile telephone or similar device while driving any motor vehicle or while supervising a holder of a provisional licence at a time when the provisional licence holder is driving a motor vehicle.

The Regulations permit use of hand-held mobile telephones whilst driving in an emergency, or whilst calling the police, fire, ambulance or other emergency service only.

The regulation specifies that any mobile telephone that is or must be held at any time while in use is a hand-held telephone. The use of an ear piece does not make a telephone hands free. To be hands free the telephone must be fixed or in a cradle.

If the phone is hands-free there is still a risk of prosecution for failing to have proper control of a vehicle under Regulation 104 of the Road Vehicles (Construction and Use) Regulations 1986 if it is used when driving. If there is an incident, the use of any phone or similar device might justify charges of careless or dangerous driving.

The School advises that all hand-held mobile telephones should be switched off whilst driving.

6.6 INTERNET TELEPHONY

The use of Skype is available to Users through a formal request to the ICT Services Helpdesk. This facility is provided for and to support teaching and learning, or for business use only and all usage must adhere to the applicable areas of School policy.

Data Protection Policy

7. INTRODUCTION AND SUMMARY

The purpose of this policy is to define the rights of individuals to privacy with regard to the processing of personal data.

In the event of a conflict between this policy and the Data Security Policy, the specific terms of this policy take precedence.

This policy forms part of the conditions of employment for employees, and is part of the contractual agreement for suppliers. All parties must read the policy completely and confirm that they understand the contents of the policy and agree to abide by it.

7.1 DATA PROCESSING

It is necessary for the School to process personal data in the normal and proper conduct of academic and business operations. Such processing will be conducted fairly and lawfully in accordance with current legislation on Data Protection.

If employees have any queries regarding the accuracy of their personal data then their queries will be dealt with fairly and impartially.

7.2 GENERAL USE OF PERSONAL DATA

The School holds data on:

- prospective, current and former pupils;
- prospective, current and former employees;
- other business and academic contacts;
- and other individuals interested in the School.

This personal data is held in a variety of formats, electronic and manual. The processing of personal data is subject to the rules laid down under the Data Protection Act (1998) and the General Data Protection Regulation (2018). The employees' personal data will be used only for proper purposes that are considered by the School to be for the benefit of the employee.

For employees this will include (but will not be restricted to) the conduct of normal business management and employment matters. The protection of employees' personal data will be governed by the provisions of the Data Protection Act (1998) and the General Data Protection Regulation (2018). Access to personal data will be restricted to those personnel to whom it is necessary for proper purposes.

The School will not sell employees' personal data to third parties. Personal data will only be transferred to third parties where this is for proper purposes related to academic and business matters, for example where this is required by professional bodies or where it is necessary for the delivery of services by third parties.

For other individuals not employed by the School this will include (but will not be restricted to) the normal conduct of academic and business relationships.

7.3 THE PRINCIPLES OF DATA PROTECTION

There are eight Data Protection principles set out under the legislation. In summary they are that personal data should be:

1. obtained and processed fairly and lawfully;
2. held and used only for specified purposes;
3. adequate, relevant and not excessive;
4. accurate and kept up to date;
5. kept only for as long as is necessary;
6. processed according to the Act;
7. held securely;
8. held within the European Economic Area.

The School is registered as a Data Controller under the legislation and will adhere to these principles and the guidelines set out by the Information Commissioner. The School's registration number is Z934173X.

7.4 DATA PROTECTION OFFICER

The School has appointed the Clerk & Treasurer as Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998 and the General Data Protection Regulation (2018).

7.5 CONSENT

The School seeks to use employees' personal data only for the purposes of legitimate interests and, where practicable, with their consent.

Pupils

It is a condition of acceptance that pupils consent to the School processing their personal data.

Employees

It is a condition of employment that employees consent to the School processing their personal data. By applying they signify their agreement for data to be processed.

Employees have the right to know what personal data the School holds about them and for this to be correct. Procedures for the management of personal data are in place and enquiries may be made as set out in this policy.

For other individuals not employed by the School, the School may gather their data during the course of normal academic and business activities. It will be used only for legitimate interests.

7.6 PUPIL INFORMATION

The School operates an associated Data Protection Policy for Pupils.

7.7 EMPLOYEE CONFIDENTIAL REFERENCES

Employees are not entitled to see references provided by the School on their behalf.

Employees may be entitled to see references about them received by the School, although this will depend on whether it compromises the privacy of a third party.

7.8 DEFINITION OF PERSONAL DATA

Personal Data is any data in which living people can be identified individually. It can take the form of electronic or manual records as well as photographic and CCTV images. It includes any facts or opinions relating to an individual, and information regarding the intentions of the data controller towards the individual and the action that will follow the processing of the data.

Sensitive Personal Data is personal data relating to an individual’s mental or physical health, race, ethnic origin, religious or political beliefs, sex life or trade union membership.

If the School holds Sensitive Personal Data about employees then this will only be disclosed with their explicit consent or if required by law.

7.9 ACCESSING PERSONAL DATA

Employees have the right to see the personal data that the School holds about them and for that data to be corrected if it is incorrect. Minor requests about employees’ personal data may be dealt with informally in the course of normal administration, at the sole discretion of the School.

If an employee wishes to make a formal request for access to their personal data then this should be made in writing to the appropriate Senior Officer. The School aims to provide the requested information within 28 days.

7.10 EXEMPTIONS

Certain data is exempted from the provisions of the Data Protection legislation which includes the following:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

7.11 ACCURACY

The School will endeavour to ensure that all personal data held in relation to all employees is accurate. Employees should notify the DPO of any changes to information held about them. An employee has the right to request that inaccurate information about them is erased.

7.12 ENFORCEMENT

If an employee believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection legislation, the employee should utilise the School grievance procedure and should also notify the DPO.

7.13 EMPLOYEE INFORMATION

Further details on the use of employee personal data may be found in the appropriate Divisional Handbook on the School intranet. All enquiries should be directed to Personnel or the Head of Department/Line Manager, as appropriate.

7.14 DATA RETENTION

The Data Protection legislation states that personal data must not be kept for any longer than is "reasonably necessary for its particular purpose".

The retention period for any document or written record of personal data will be assessed with regard to its: (1) particular use; (2) content; and (3) importance before it may be discarded. Employees must seek permission from Senior Management before such data is discarded and if this is deemed appropriate it will be discarded in a secure manner.

Minimum retention periods:

- Personnel documents - keep for a minimum of six years from the end of employment
- Pastoral documents - keep for a minimum of six years from the date the pupil leaves School
- Health and safety records - documents such as accident books and records of reportable injuries must be kept for a minimum of six years
- Statutory Financial and Taxation records – documents will be kept for a minimum of seven years from the end of the period to which they relate.

Data Security Policy

8. SECURITY AND PRIVACY

The School employs various measures to protect the security of its ICT resources and its Users' accounts. Users should be aware, however, that the School cannot guarantee security or confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly. It is not permitted for Users to share their access to School systems with anybody else. The one exception to this is to facilitate a lesson review situation at interview. In these special circumstances the reviewing member of staff may share their access with the interviewee but he/she must be present for the whole time the interviewee is using their shared access and he/she must log off the interviewee immediately the lesson review session ends.

Users should also be aware that their use of School ICT resources is not completely private. ICT Services actively monitors usage of School ICT resources. The normal operation and maintenance of the School's ICT resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service.

ICT Services, upon request from the Senior Officers, will monitor the activity and accounts of individual Users of School ICT resources, including individual login sessions and the content of individual communications, without notice, when:

- it reasonably appears necessary to do so to protect the integrity, security, or functionality of School or other ICT resources or to protect the School from liability;
- there is reasonable cause to believe that the User has violated or is violating any School policy;
- an account appears to be engaged in unusual or unusually excessive activity or in activities not permitted by law.

The School may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to senior personnel at the School or law enforcement agencies and may use those results in School disciplinary procedures.

8.1 DATA DEFINITION

For the purposes of this policy, data refers to all information stored in a digital format and held on School ICT systems or equipment.

The use of the term “data” also includes all images taken by a User and stored on School media, including memory cards. Storage and transfer of images of pupils must be in compliance with all School policies, including the safeguarding policies, regardless of whether they have been approved by parents or guardians for the public domain.

8.2 SUMMARY OF INDIVIDUAL RESPONSIBILITY

All Users accessing School data must do so only in conformance with this policy.

- Users are responsible for maintaining the security and confidentiality of data in their possession, such as hardcopy reports or data downloaded to their workstations or cloud storage. Users must report to the Head of ICT Services any known breach of application or system security.

- Users may not remove, copy or transmit sensitive or personal data from the School or authorised premises unless authorisation has been obtained from a Senior Officer or the Data Owner, as appropriate. This includes data and images stored on removable media, portable devices or cloud storage. Preference should be given to the use of the School secure remote access systems for such use; if this is not possible, encrypted removable media devices must be used and stored in a secure location.

- The use of School ICT resources is subject to the requirements of legal and ethical behaviour. Users of School ICT resources must comply with national laws, School rules and policies, and the terms of applicable contracts including software licenses

- Users must securely delete sensitive or personal data when it is no longer required, in compliance with the Data Protection Act (1988) and the General Data Protection Regulation (2018.

- Users who engage in electronic communications with persons in other countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks.

- Users are responsible for obtaining necessary authorisation before using School ICT systems. Users are responsible for any activity originating from their accounts, which they can reasonably be expected to control. Persons other than those to whom they have been assigned by the network or system administrator may not use accounts and passwords. In cases when unauthorised use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the appropriate system administrator.

- Users must not use ICT resources to gain unauthorised access to remote computers or to impair or damage the operations of computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or ‘sniffing’ communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not permitted.

8.3 DATA OWNERSHIP

All systems will have a Data Owner, who will take responsibility for that system and its associated data. The Data Owner, in conjunction with the Head of ICT Services, will define the security, authentication and authorisation requirements and procedures for each system.

It is also the Data Owner’s responsibility to:

- ensure suitable procedures are in place to maintain access to School systems in exceptional circumstances;

- ensure any confidential data stored off-site is securely stored to a level at least commensurate to the security of the data stored on-site and complies with all relevant UK legislation.

Data Owners can be permanent or temporary roles, for example a trip leader would be the Data Owner for the duration of the trip.

8.4 PREVENTING THE SPREAD OF MALICIOUS SOFTWARE (VIRUSES)

Any ICT equipment, regardless of ownership, must have up-to-date Anti-Virus scanning software operating before it can be connected to the School network via any permitted means as detailed in the School ICT Equipment and Systems Policy. Notification of a virus on either a School ICT computer or device or a personal device connected to the School wireless network, must be immediately reported to the ICT Services Helpdesk and further use of the device suspended until a member of ICT Services confirms its safe use.

Concerns about antivirus protection should be discussed with ICT Services who can assist with providing suitable antivirus software.

8.5 DATA BACK-UP AND RECOVERY PROCEDURE

All employees must ensure the security and maintain backups of their own data, when stored on a laptop or other portable device.

The following backup procedure is undertaken by ICT Services. All backup tapes are stored on site in a fire resistant safe.

- Daily incremental backups onto tape.
- Weekly Data Full backup onto tape.
- Monthly full backup onto tape.
- Annual backup. Retained for 7 years and taken at the end of the academic year.
- Server images are taken daily and stored on ‘network attached storage’ (NAS).

8.6 MANAGING SYSTEMS FOR EMPLOYEES LEAVING

When an employee becomes no longer employed by the School, a member of the Personnel department will inform the ICT Helpdesk of their leaving date, from which time their network User account will normally be suspended and all access to School systems and data will be revoked.

It is the responsibility of the individual’s Head of Department to ensure that any data relevant to the operation of the department is transferred from the individual’s work folder to an alternative and appropriate file storage location prior to their leaving date.

8.7 MANAGING SYSTEMS FOR PUPIL LEAVERS

When a pupil leaves the School, the appropriate Head's secretary will inform the ICT Helpdesk of their leaving date, from which time their network User account will normally be suspended and all access to School systems and data will be revoked. All content from their work area will be deleted following an archive procedure to permit restoration of data for returning pupils if required.

It is the responsibility of the pupil to take a copy of their data prior to their leaving date.

8.8 MAINTAINING CONFIDENTIALITY OF RESTRICTED DATA

In the course of accessing data or information, a User might access restricted information within the particular database. It is the responsibility of the Data Owner to ensure that all individuals with access to restricted data are aware of the confidential nature of the information and the limitations in terms of disclosure that apply. Any questions regarding Data Protection should be addressed to the Clerk and Treasurer in her role as the School's Data Protection Officer.

- Users must not access confidential information without gaining the appropriate permission to do so.
- Users must ensure that ICT equipment is logged out when left unattended at any time. It is prohibited to leave any ICT device displaying confidential data unattended at any time.
- Authorised Users must not allow access to School systems by unauthorised Users and must ensure that User information including passwords are not made available or accessible by unauthorised Users.
- When accessing restricted information, Users are responsible for maintaining its confidentiality. Having been granted authentication credentials to access a system assumes that Users will maintain confidentiality over appropriate information without exception.
- The release of restricted data without the express approval of one of the Senior Officers or the Data Owner, as appropriate, is not permitted.
- Unauthorised release of restricted information may result in disciplinary action. All operational matters involving employees will be reviewed by the employee's line manager or the School Senior Officers, as appropriate.
- Transgressions involving pupils will be reviewed by the Senior Officers.

8.9 DATA STORAGE

Users must ensure that all confidential information is stored either within their personal secure work folder or the secure shared file storage. All portable devices and removable media, including memory cards, must be securely stored at all times. Once the data has been transferred or is no longer required, the media must be re-formatted. It is the User's responsibility to ensure the security of the data on such media at all times.

8.10 DATA DISPOSAL

All data should be properly disposed of when it has exceeded its required retention period as defined in the School's Data Protection Policy. This includes output such as paper listings, CDs, backup tapes, and DVDs.

8.11 PHYSICAL SECURITY

ICT Services and the Estates department will ensure the physical security of the server room, which will be accessible to Senior Officers and authorised ICT Services and Estates employees only.

ICT equipment within School must only be used by authorised Users.

Physical security of the building is the responsibility of the Estates department in conjunction with all employees.

8.12 NETWORK SECURITY

The security of the network is the responsibility of ICT services and all School system Users. ICT services will ensure that the network is accessible by authorised Users only.

Access to ICT equipment, including portable ICT equipment and smart phones, which have open access to School data and communications systems must be authenticated using a Username and password, passcode or other appropriate authentication mechanism; regardless of ownership.

All ICT equipment owned by Bolton School may be recalled for audit at any time.

Users must not attempt to implement their own network infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to ICT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS. Exceptions to this policy must be coordinated with the Head of ICT Services.

Users must not provide unsupervised access to School systems via any method to anyone. All access to the network must be approved by the Head of ICT Services. Remote access for support must be provided using a secure service. Any access to the School network must never be left unattended.

If Users suspect or become aware that a security problem may have arisen in relation to their computer or device, or any other computer or device, they should immediately inform the Head of ICT Services.

8.13 LEGAL ISSUES

The Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allow employers to investigate or detect the unauthorised use of its telecommunication system, including internet use.

The Data Protection Act 1998 and the General Data Protection Regulation (2018) will also apply if the monitoring of internet use involves the processing of information from which an individual can be identified. The Employment Practices Data Protection Code (PDF format, 5.5MB)

8.14 DATA PROTECTION ACT

The Data Protection Act 1998 and the General Data Protection Regulation (2018) regulates the use of personal data. Any User putting information (including photographs) onto any Bolton School ICT system or the Internet, containing personal data other than their own must have the express written consent of the individual to whom the personal data relates, if it identifies them or could be used to do so. Unless legally required to do so, Users must not disclose personal information to anyone unless they have written authority from either the Clerk and Treasurer or the Data Owner, and the individual concerned.

If Bolton School fails to meet these obligations, the School could be fined and found guilty of a criminal offence. In certain circumstances, Users may also be fined and could be personally criminally liable.

8.15 COMPUTER MISUSE ACT

The Computer Misuse Act 1990 applies to everyone who uses a computer or computer system. It is a criminal offence to seek unauthorised access or modifications of any computer material.

9. ICT POLICIES ACCEPTANCE FORM

I have read, understood, and will abide by the terms and conditions of the Bolton School ICT Policies. I further understand that any violation of the regulations is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked; School disciplinary action may be taken and/or appropriate legal action.

By signing this acceptance I acknowledge that I have read the policies listed below.

Access to the School network will be enabled after this acceptance form is signed.

Tick the boxes below to confirm that you have read and accept and consent to the terms and conditions of the Bolton School ICT Policies:

1. General Conditions □
2. Acceptable Use of ICT Equipment and Systems Policy □
3. Acceptable Use of Internet and Social Networking Policy □
4. Acceptable use of Email Policy □
5. Acceptable Use Policy for iPads & Laptops □
6. Acceptable Use Policy for Telephones, Smart Phones, Mobile Phones & Devices and Internet Telephony □
7. Data Protection Policy □
8. Data Security Policy □

User Name: ______________________________

User Signature:______________________________

Date: ___/ ___/ ___

Data Protection Policy – Pupils

10. GENERAL STATEMENT OF THE SCHOOL'S DUTIES

The School is required to process relevant personal data regarding pupils and their parents and guardians as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this policy any reference to pupils includes current past or prospective pupils.

10.1 DATA PROTECTION CONTROLLER

The School has appointed the Clerk & Treasurer as Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act (1998) and the General Data Protection Regulation (2018).

10.2 THE PRINCIPLES

The School shall so far as is reasonably practicable comply with the Data Protection Principles (”the Principles”) contained in the Data Protection legislation to ensure all data is:-

1. obtained and processed fairly and lawfully;
2. held and used only for specified purposes;
3. adequate, relevant and not excessive;
4. accurate and kept up to date;
5. kept only for as long as is necessary;
6. processed according to the Act;
7. held securely;
8. held within the European Economic Area.

10.3 PERSONAL DATA

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data of pupils, their parents or guardians as part of its operation. This personal data may include (but is not limited to); names and addresses, bank details, academic, disciplinary, admissions and attendance records, references, examination scripts and marks.

10.4 PROCESSING OF PERSONAL DATA

Consent may be required for the processing of personal data unless the processing is necessary for the School to undertake its obligations to pupils and their parents or guardians. Any information, which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

10.5 SENSITIVE PERSONAL DATA

The School may, from time to time, be required to process sensitive personal data regarding a pupil, their parents or guardians. Sensitive personal data includes medical information and data relating to religion, race or criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will generally be required in writing.

10.6 RIGHTS OF ACCESS

Individuals have a right of access to information held by the School. Any individual wishing to access their personal data should put their request in writing to the DPO. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 1 month.

You should be aware that certain data is exempt from the right of access under the Data Protection legislation this may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts.

The rights under the Data Protection legislation are the individual's to whom the data relates. The School will however in most cases rely on parental consent to process data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is reasonable in all the circumstances to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted.

The School will only grant the pupil direct access to their personal data if in the School's reasonable belief the pupil understands the nature of the request.

Pupils agree that the School may disclose their personal data to their parents or guardian, except for where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian. In such circumstances the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils, or where there is a court order to do so.

10.7 EXEMPTIONS

Certain data is exempted from the provisions of the Data Protection legislation which includes the following:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

10.8 DISCLOSURE OF INFORMATION

The School may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The School confirms that it will not generally disclose information unless the individual has given their consent, or one of the specific exemptions under the Data Protection legislation applies.

However, the School does intend to disclose such data as is necessary to third parties for the following purposes:

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend;
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend;
- To publish the results of public examinations or other achievements of pupils of the School;
- To disclose details of a pupil’s medical condition where it is in the pupil’s interests to do so, for example for medical advice, insurance purposes or to organisers of School trips.
- For public examination purposes, examination results data analysis or where malpractice is suspected, where relevant personal data may be shared in accordance with JCQ policies and procedures.
  Parents may follow this link to see the JCQ Privacy Notice:
  https://www.jcq.org.uk/exams-office/information-for-candidates-documents/information-for-candidates---privacy-notice

Where the School receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

10.9 USE OF PERSONAL INFORMATION BY THE SCHOOL

The School will, from time to time, make use of personal data relating to pupils, their parents or guardians in the following ways:

- To make use of photographic images of pupils in School publications and on the School website. However, the School will not publish photographs of individual pupils with their names on the School website without the express agreement of the appropriate individual.
- For fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, including transferring information to any association society or club set up for the purpose of establishing or maintaining contact with pupils or for fundraising, marketing or promotional purposes.

Should you wish to limit or object to any such use please notify the Heads or the DPO in writing.

10.10 ACCURACY

The School will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

10.11 SECURITY

The School will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the Data Protection legislation. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons.

All data held on School ICT systems will be held in compliance with the School's Data Security Policy.

10.12 ENFORCEMENT

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection legislation, they should utilise the School complaints procedure and should also notify the DPO.

Pupil Acceptable Use Guidelines for Social Networking

11. SELF-PUBLISHING AND SOCIAL MEDIA GUIDELINES: PUPILS

These Guidelines are for pupils who use social media including blogs, podcasts, wikis and social networking sites for online communication and collaboration as part of their learning activities.

11.1 PUBLISHING GUIDELINES

Publishing work or ideas on the Internet is a very public activity. You should think carefully about anything you publish. Even if you delete something after you have published it, it can be found on the web for years afterwards. You shouldn't publish anything you wouldn't be comfortable with anyone viewing e.g. parents, teachers, future employers.

11.2 BE SAFE

Anyone can access the Internet and view what you write on a blog or wiki. Even if your page is 'protected' there is nothing to stop your friends from copying your material and placing it elsewhere on the web. It is important to respect your privacy. Use your first name only and do not use pictures of yourself. If you wish to have an image associated with your blog, use a picture of something that represents you. Don't give out any personal information about yourself or anyone else.

11.3 BE MINDFUL OF WHAT YOU SAY

You are responsible for anything that is posted in your name. Always use appropriate language and remember that how you say something is as important as what you say. Avoid exaggeration, provocation and sarcasm in the language you use.

When podcasting, consider what you are presenting and how you are presenting it. Could you be misunderstood? Be clear in the message you are trying to convey.

11.4 BE RESPECTFUL TO OTHERS

When writing on your blog or wiki or if you are commenting on others, always make sure what you write is fair and accurate.

When podcasting, do not record any person without his or her consent and awareness. You must have the consent from every individual whose voice can be heard on your podcast. Start each audio recording by identifying everyone present by their first name only.

Other bloggers and podcaster will love to hear what you think of their work. If you want to make some constructive criticism why not try giving two stars and a wish (two positive comments and one thing you think could improve).

You must not

- Harass or bully fellow pupils or members of staff;
- Add teaching staff as friends;
- Communicate with staff except through School learning systems;
- Publish any information about School staff;
- Publish any information which may damage the reputation of the School.

11.5 SECURITY AND IDENTITY THEFT

You should be aware that social networking websites are a public forum, particularly if you are part of a "network or group". You should not assume that entries on any website would remain private.

You must also be security conscious and should take steps to protect yourself from identity theft, for example by restricting the amount of personal information that you out.

Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

In addition, you should:

- ensure that no information is made available that could provide a person with unauthorised access to the School and/or any confidential information
- refrain from recording any confidential information regarding the School or members of staff on any social networking website.

Pupil iPad Acceptable Use Policy

12. PARENTS AND PUPILS MUST SIGN AND RETURN COPIES OF THE 'PUPIL IPAD ACCEPTABLE USE POLICY FORM' (FOUND AT THE END OF THIS POLICY) BEFORE THE IPAD IS ISSUED.

The iPad remains School property and all Users will follow these procedures alongside any other relevant Acceptable Use Policies. Pupil iPads will be labelled in the manner specified by the School so that they are easily identifiable. Each iPad will be asset tagged and be recorded on the School inventory.

Each iPad will also have a label on the outside of the case, containing the asset ID and a space for the pupil to write their name.

The use of the School's technology resources is a privilege, not a right. The privilege of using the technology resources provided by Bolton School is not transferable or extendible by pupils to people or groups other than pupils at the School and terminates when a pupil no longer attends the School.

All iPad Users should be aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges may be terminated, access to the School technology resources may be denied, and the appropriate disciplinary action shall be applied. *Violations may result in disciplinary action up to and including suspension/expulsion for pupils.*

Bolton School reserves the right to confiscate and search an iPad to ensure compliance with this Acceptable Use Policy.

12.1 IN ORDER TO ENSURE THAT THE IPAD REMAINS IN GOOD WORKING ORDER AND IN A SATISFACTORY CONDITION, THE FOLLOWING GUIDELINES MUST BE HEEDED:

- Pupils are responsible for the general care of the iPad they have been issued by the School. IPads which are broken or fail to work properly must be taken to the School office for an evaluation of the equipment.
- Do not remove the iPad from its protective case.
- Only use a clean, soft cloth to clean the screen; do not use cleansers of any type.
- The iPad screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen. Therefore, do not lean on the top of the iPad when it is closed. Do not place anything near the iPad that could put pressure on the screen. Do not place anything in the carrying case that will press against the cover.
- Cords and cables must be inserted carefully into the iPad to prevent damage.
- The iPad and its case must remain free of any writing, etchings, scratching, drawing, stickers, or labels that are not provided by Bolton School when the iPad is handed out.
- IPads should not be used near food or drinks, which might spill on them.

- IPads must never be left in an unlocked locker, unlocked car or any unsupervised area. Unsupervised areas include the School grounds and campus, the dining room, computer rooms, form rooms, the Riley Centre, library, changing rooms and corridors. Any iPad left in these areas is in danger of being stolen. If an iPad is found in an unsupervised area, it will be taken to the School office. Violation~~s~~ of this rule may result in loss of iPad privileges and/or other privileges.
- The iPad must not be left in a place that is experiencing extreme hot or cold conditions (e.g. car in summer or winter). Extreme heat will damage the unit itself. Extreme cold will cause severe screen damage.
- Outside School, the iPad must be carried in a bag, rather than openly in your hand. If there are other belongings in the bag, these must be kept to a minimum to avoid placing too much pressure and weight on the iPad screen. Do not carry the iPad in a bag containing any liquids which might spill on to the iPad and cause damage.
- Do not disassemble any part of any iPad or attempt any repairs.

12.2 THE FOLLOWING RULES APPLY IN SCHOOL ABOUT THE IPAD'S CONTENT AND USE:

- You will be personally responsible for any content on your device and for any use of your device.
- Passwords must be used to restrict access to your device; you are personally responsible for knowing your own password and ensuring that you do not pass it to others.
- If internet game apps are to be used in School, extreme care should be taken when using any associated chat room functionality. If in doubt about any aspect of an internet game app, you should ask a member of staff for their advice.
- Apps required by the School will be installed and these educational apps will have priority on the device. If a User runs out of space on their device we may need to uninstall personal apps in order to install educational apps required by School.
- In School and at home, your iPad will come under the control of a Device Manager. This will govern what you can or cannot do with your iPad.

12.3 RULES FOR IPAD APPLICATIONS

- The software/apps originally installed by the School must remain on the iPad in a usable condition and be easily accessible at all times. From time to time the School may add software applications for use in a particular course. The licenses for this software require that the software be deleted from iPads at the completion of the course. Periodic checks of iPads will be made to ensure that pupils have not removed required apps and have deleted software if required.
- Pupils are allowed to load age appropriate extra software/apps on their iPads but, should the memory on the iPad become full, then the School-required apps will have priority and this may require the User installed software to be uninstalled.
- Pupils must not allow younger pupils to access software/ apps on the iPad which are inappropriate for their age group; for example, the Twitter and Facebook apps must not be used by members of Years 7 and 8 as they are not age-appropriate for some or all of the pupils in those year groups.

- If technical difficulties occur, the iPad will be restored to its default settings. The School does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.
- Upgrade versions of licensed software/apps are available from time to time. Pupils will be required to allow the installation of software updates to their iPads.
- Pupils may be selected at random to provide their iPad for inspection.
- Individual Users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the School.

12.4 USING THE IPAD AT SCHOOL AND AT HOME

- IPads must be taken home each evening and brought to School every day. If you do not need to take your iPad home to complete your studies one evening, then you must leave it in your locked locker overnight.
- Pupils must bring their iPad to all classes, unless specifically instructed not to do so by their teacher.
- If pupils leave their iPad at home, they are responsible for getting any School work completed as if they had their iPad present.
- If a pupil repeatedly leaves their iPad at home, an appropriate sanction will be applied.
- IPads must be brought to School each day in a fully charged condition.
- Pupils need to charge their iPads each evening.
- If a pupil repeatedly fails to charge his or her iPad at home, an appropriate sanction will be applied.
- In cases where use of the iPad has caused batteries to become discharged, pupils may be able to connect their iPads to a power outlet in exceptional circumstances and under the direction of the teacher.
- The iPad should be transported to and from School, and between lessons, in a School bag. At all other times it should be kept in a locker. IPads must not be left in unattended bags, including in bag storage areas at any time.
- If the Pupil is temporarily excluded from School for a period of time, including where the Headmaster or Headmistress is considering a case to exclude him or her permanently, or where the parent is appealing a decision to exclude, then the Pupil may be asked to hand in his/her iPad during such a period. In such cases, the submission of the iPad is a neutral act and is not designed to suggest that the Pupil will be required to leave the School permanently in due course. During such times, the Pupil will be given access to work and educational support via other means.

12.5 PUPILS WILL DO THE FOLLOWING TO COMPLY WITH THIS POLICY

- Use iPads/computer/devices in a responsible and ethical manner (see prohibited activities).
- Obey general School rules concerning behaviour and communication that apply to iPad/computer use.
- Use all technology resources in an appropriate manner so as not to damage School equipment. This "damage" includes, but is not limited to, the loss of data resulting from

delays, non-deliveries, miss-deliveries or service interruptions caused by the pupil's own negligence, errors or omissions.

- Help the School protect its computer system/devices by contacting an administrator about any security problems they may encounter.
- Monitor all activity on their account(s).
- Turn off and secure their iPad after they have finished working to protect their work and information.
- Ensure that, if they receive email containing offensive, inappropriate or abusive language/ content or in which the subject matter is questionable or makes them feel uncomfortable, print a copy and give it to the relevant member of the pastoral staff to investigate.
- Ensure that, when they send an email, they abide by the School's acceptable use policies.
- Ensure that they do not send an email to a member of staff unless specifically invited to do so by the relevant member of staff e.g. in response to a staff email to them.
- Ensure that they do not use emails to inform staff of occurrences (e.g. future absences) which they ought, out of common courtesy, to say face to face to the member(s) of staff concerned.
- Users should be aware of and abide by the guidelines set out by School policies.

12.6 PROHIBITED ACTIVITIES INCLUDE:

- Any action that violates existing School policy or public law.
- Any attempt to Access Inappropriate Materials – all material on the iPad must adhere to the ICT Acceptable Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, bullying, pornographic, obscene, or sexually explicit materials.
- Use of the School's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Sending mass or inappropriate e-mails – spamming.
- Use of the camera and microphone is strictly prohibited in School unless specific permission is granted by a teacher on a specific occasion to do so.
- At other times Users must use good judgment when using the camera. The User agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of a camera in the toilets or changing rooms, regardless of intent, will be treated as a serious violation.
- Use of social media sites is prohibited for all Users below the appropriate age to access the site.
- Images of other people may only be made with the permission of those in the photograph and only if allowed under the Behaviour Management Policy of the relevant School.
- Posting of images/movie on the internet into a public forum is strictly forbidden, without the express permission of the Teacher.
- Misuse of Passwords, Codes or other Unauthorized Access.
- Any User caught trying to gain access to another User's accounts, files or data will be subject to disciplinary action.
- Malicious Use/Vandalism – any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Jail breaking – the process which removes any limitations placed on the iPad by Apple.

- Pupils must not use their iPad in School corridors, on their journeys to and from School (including coaches) or outside of School buildings (unless with a Teacher's express permission).

12.7 PARENTAL LIABILITY FOR THE IPAD

- I understand that my child is borrowing the iPad from School and that the iPad must be returned to School upon demand. When requested, it must be returned in good mechanical and cosmetic condition (allowing for fair wear and tear) including all components and accessories such as AC adaptors, batteries and cases.
- The School will be responsible for repairing iPads which malfunction.
- I will ensure my child takes reasonable care of the iPad at all times, does not wilfully neglect it and does not leave it in the custody of a third party or allow anyone not so authorised by School to use it.
- I will immediately upon delivery of the iPad, inspect it and notify the School Office of any defect. In the absence of such notification it shall be conclusively presumed that the iPad is in good working order and condition.
- I will notify the School Office or Head Teacher and also by email to helpdesk@boltonSchool.org immediately if the iPad is lost, stolen or damaged. This is vital to secure the iPad and, in certain circumstances, iCloud can be used to track stolen iPads.
- I will ensure my child does not leave the iPad unattended in an unlocked vehicle, in the open air, in a public place or in any outbuilding, i.e. to ensure it is kept within sight or control at all times when in these places.
- If the iPad is left unattended in a locked vehicle, then it will be in the locked boot of a saloon car, or concealed under the rear parcel shelf of a locked hatchback car, or concealed in the spare wheel or other closed compartment of a locked estate car. For any insurance claim made by the School to be valid, proof of forcible entry would be required.
- In the event of theft, accidental damage or destruction of all or part of the iPad and its associated components and accessories including the case, or where the iPad is returned and deemed unusable, I agree to pay to School a £50 penalty. In the event of theft, a crime number will need to be provided.
- If the iPad is lost, where no crime number is obtainable, I will be liable for the full cost of a replacement iPad.
- Any unpaid penalty may be added to my contractual School Fee arrangements and collected under the terms and conditions imposed by the School Fee Contract and/or deducted from my pupil deposit balance held by School.

Parental Agreement

- I have read and understood the Bolton School Pupil iPad Acceptable Use Policy.
- I agree to abide by the stated rules.
- I understand that I am responsible for managing my child's use of this device at home.

Name of Pupil ____

Name of Parent or Guardian____

*Signature of Parent or Guardian ____________________________ Date__________

**This form must be signed by someone who has parental responsibility as defined by the Children Act 1989.*

12.8 PUPIL PLEDGE FOR IPAD USE

	I will take good care of my iPad.		I will never lend my iPad to others.
	I will never leave the iPad unattended outside the School building.		I will tell a teacher if I see pages or emails that are offensive.
	I will not switch off the ‘Find my iPad’ feature on my device.		I will not use my iPad to share copyrighted files.
	I will only access the iPad and network when given consent by my teacher.		I will not give out personal information on line or in emails.
	I will only send emails to the people I know or who are approved by my teacher.		I will ensure that any emails or blog posts are polite.
	I will only use my official School email account and will not add other email accounts to my iPad		I will copy and use material as allowed by copyright legislation. I will check with my teacher if I am unsure.
	I will know where my iPad is at all times.		I will charge my iPad’s battery every night.
	I will keep food and drinks away from my iPad since they may cause damage to the device.		I will never share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.
	I understand that my iPad is subject to inspection at any time without notice.		I agree to abide by the statements of this iPad acceptable use policy.
	I will only use the camera or the microphone when my teacher tells me to.		I will use my iPad in ways that are appropriate.
	I will not disassemble any part of my iPad or attempt any repairs.		I will protect my iPad by only carrying it whilst it is in a case.
	School rules forbid photography or videoing in School or on School activities, including the coach.		When travelling to and from School and between lessons my iPad will remain inside my School bag. At all other times it will be left securely in my locker.

Pupil agreement

- I have read and understood the Bolton School Pupil iPad Acceptable Use Policy.
- I agree to abide by the stated rules.
- I accept that any infringement of these rules could result in the cancellation of my School iPad/computer privileges, and depending on the situation the usual range of School sanctions.

Pupil ______________________________________ Form _________
(Please print clearly)

Pupil signature ____________________________ Date __________________

Pupil ICT Acceptable Use Policy

13. USE OF ICT FACILITIES ON SCHOOL PREMISES IS A PRIVILEGE NOT A RIGHT

The School ICT network and resources are made available to pupils to enhance their educational opportunities. The School has a responsibility to ensure that it maintains the integrity and performance of ICT resources for this purpose. School ICT facilities are provided to pupils solely for their studies and the School reserves the right to withdraw them at any time. All use of School ICT equipment and systems is logged and monitored; violations of this policy will be disciplined on an individual basis in line with the School behaviour policies.

A personal School e-mail account is provided to all pupils from Year 3 upwards. It is every pupil's responsibility to use this facility appropriately and solely to further their studies.

Sixth Formers may, at their own risk, bring in a personal wireless device such as a tablet or notebook. These may not be connected to the School's wireless network unless by prior arrangement with the Head. It is not permitted for pupils to charge their own personal device in School.

13.1 PUPILS USING SCHOOL ICT FACILITIES MUST ABIDE BY THE FOLLOWING RULES:

Protect your own work:

- You must protect your own work by keeping your network password secret and not sharing it with other pupils. You must always log off your computer before leaving it unattended for periods of time to prevent your files being accessed by someone else. It is your responsibility to backup your own work.

Protect the School ICT network and resources:

- You must not deliberately gain unauthorised access to School ICT resources or impair or damage the operation of School ICT resources, nor must you allow anyone else to do so. You must be pro-active in your use of anti-virus software and make every effort not to introduce any viruses to the School network. Pupils are not permitted to physically connect any ICT equipment to the School network.

Show respect for others:

- You must never download or upload any material to or from any ICT device, regardless of ownership, which could be considered defamatory, immoral or offensive. **Cyber-Bullying is entirely unacceptable** and will be dealt with severely following the Schools' anti-bullying policy.

Uphold the law:

- You must not use the School ICT facilities for any activity that may reasonably be regarded as unlawful or potentially so. Any pupil who violates the 'Computer Misuse Act 1990', the

‘Copyright, Designs and Patent Act 1988’ and other associated Acts of Parliament will be disciplined following School procedures.

Protect the School:

- You must protect the reputation of the School by not posting anything online that could bring the School or any members of staff into disrepute.

Stay safe online:

- You must not follow or add personal accounts of Staff, volunteers or other adults you have known through being a Pupil at Bolton School as friends on Social Networking sites or communicate with staff electronically except through School ICT systems. This includes the first year after you leave School. You must protect yourself by never publishing any personal information about yourself and your activities online. If you have seen or are involved in anything online which concerns you, you must report it to your form tutor.

Pupils will only be able to use the School ICT facilities if they and a parent or legal guardian have signed the following agreement and returned this form to School.

13.2 PUPIL STATEMENT

- I have read and understood Bolton School's Pupil ICT Acceptable Use Policy.
- I agree to abide by the stated rules.
- I accept that any infringement of these rules could result in the cancellation of my School ICT privileges, or at worst, expulsion.

Pupil: ___________________________________ **Form** *(if known):* _________
(please print)

Pupil signature: __________________________ **Date: _________________**

*13.3 PARENTAL STATEMENT**

- I have read and understood Bolton School's Pupil ICT Acceptable Use Policy.
- I wish my child to have access to the Bolton School ICT network and systems as detailed above under these conditions.

Name of Parent or Guardian: ______________________________
(please print)

Signature of Parent or Guardian: _______________________ **Date: ______________**

Please return this slip together with the completed Parent Contract.

Internet and e-mail access will only be granted on the return of the signed slip.

* Please note that this form must be signed by someone who has parental responsibility as defined by the Children Act 1989. Under this Act parental responsibility is defined as follows:

- ♦ If parents are married, separated or divorced, both parents have parental responsibility on an equal basis.
- ♦ If parents are unmarried, only the mother has parental responsibility unless the father has obtained it by formal agreement or through a court order.
- ♦ Other people (step-parents, grandparents etc) do not have parental responsibility unless they have a court order (e.g. adoption or residence order) or have taken responsibility as legal guardian.