Tiverton Academy

ICT ACCEPTABLE USE AND E-SAFETY POLICY

Valid From Date	Next Review Date
September 2018	September 2019

1 Introduction

The purpose of this document is to ensure that all users (staff, governors, secondments, visitors etc.) of Tiverton Academy's computing facilities are aware of policies relating to their use. Effective and proper use of information technology is fundamental to the successful and efficient running of Tiverton Academy. However, misuse of information technology - in particular misuse of e-mail and access to the Internet - exposes Tiverton Academy to liability and is a drain on time and money. It is critical that all users read and understand this document and make themselves aware of the risks and exposure involved.

It is the responsibility of all users of Tiverton Academy computing facilities to be aware of, and follow all Tiverton Academy ICT policies and guidelines and to seek advice in case of doubt. Tiverton Academy's ICT policies are published on the Staff Intranet under the Policies section.

This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes. Tiverton Academy will provide notice of these updates to your official school email address or in writing.

Tiverton Academy encourages the use of school computing facilities for the mutual benefit of its staff, pupils and community. Similarly the regulations that constitute this policy seek to provide for the mutual protection of Tiverton Academy and the rights of its staff, pupils and community.

2. E-Safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection. The school has an E-Safety Leader. The current designated person for E-Safety is Debbie Norbury and Jack Bertuello.

Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed regularly

2.1 Protecting Individual User Profiles

It is the responsibility of all users issued with a username and password to keep these details secure and not allow other's to use your Individual User Profile.

It is essential that strong passwords are used. Passwords should be changed regularly or immediately if compromised.

Staff must ensure that their device is logged out or locked before leaving it unattended. This is especially important due to the access to sensitive data, pupil data, personal data that could be achieved by leaving a computer unsecured.

Users are required to ensure that personal/sensitive data is kept securely as per the provisions of the Data Protection Act 1998.

2.2 Cyber-Bullying

In line with the school's anti bullying policy, the school will not tolerate bullying and will act swiftly to resolve any incidents of Cyber-Bullying. Further details can be found in the school's anti bullying policy.

What Is Cyber-Bullying?
"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself."[1]

Cyber-bullying is the use of technology, commonly a mobile phone or the internet, deliberately to upset someone else. It can be used to carry out all the different types of bullying; an extension of face-to-face bullying. It can also go further in that it can invade home/personal space and can involve a greater number of people. It can take place across age groups and school staff and other adults can be targeted. It includes: threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images and manipulation.

Reporting Cyber-Bulling

The Head teacher, E-Safety Leader, designated members of staff for Child Protection, and designated Governor for Child Protection will:

- Ensure staff can recognise non-verbal signs and indications of cyber-bullying.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
- Publicise to all members of the school community the ways in which cyber-bullying can be reported.

3. Computing facilities

Access to school computing facilities is managed by an appointed by the Senior Leadership Team. Use of any of Tiverton Academy's computing facilities is at the discretion of Tiverton Academy.

3.1 Definition

The phrase 'Computing Facilities' as used in this policy shall be interpreted as including any computer hardware, mobile device or software owned or operated by Tiverton Academy.

3.2 Ownership

Computing facilities owned by Tiverton Academy and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Tiverton Academy. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

3.3 Monitoring

Tiverton Academy reserve the right to monitor, log and record all activity on electronic devices owned by Tiverton Academy whilst on or offsite.

Whilst accessing services provided by Tiverton Academy, such as our website and staff intranet, all activity will be logged, along with the IP address.

In maintaining the security of school owned devices, some devices may transmit their location back to our monitoring systems.

3.4 Desktop Computers

Desktop Computers are a critical asset to Tiverton Academy and must be managed carefully to maintain security, data integrity and efficiency. Users must consult the Senior Leadership Team before installing any software.

All users have access to appropriate areas on Tiverton Academy's network for the secure storage of valuable files. No files should be stored locally on Desktop Computers. It is advisable that all files are saved to your H: drive or the relevant area on Tiverton Academy's intranet.

Desktop Computers include the CPU/hard-drive unit and monitor, both of which should not be disconnected or relocated without prior permission from the Senior Leadership Team.

3.5 Laptops

Laptops are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of Tiverton Academy systems and data procedures, passwords or authentication devices for gaining remote access to Tiverton Academy systems must not be stored with the computer. This includes the saving of passwords into remote access software.

Unless your loan agreement states your laptop is encrypted, no confidential data can be stored on it.

If the Laptop is lost or stolen the Senior Leadership Team must be notified as soon as possible and a report made to the police.

3.6 Handheld and Mobile Devices

Handhelds and mobile devices, including tablets and mobile phones, are at high risk from theft due to their size and nature of usage. Because some of these devices have usage tariffs attached to them, loss of the device can expose Tiverton Academy to a large liability through fraudulent use. It is therefore vital that staff are vigilant in caring for their security.

Staff should take care to keep these devices concealed when not in use and to be conscious of onlookers who may be targeting devices for theft. In the event that a device is stolen, Staff will be expected to report the theft to the police, obtain an incident number and contact the Senior Leadership as soon as possible.

If it has a usage tariff, such as a mobile phone, the staff member will ensure the mobile service is suspended, by calling the relevant network provider. The information, including the network provider and lost and stolen number will be shown on your copy of the loan agreement issued to you.

Users of mobile devices must not change technical settings. Such changes often cause inadvertently high billing charges or other substantial loss of information or productivity. Staff who change the configuration of their devices, which causes abnormal billing or other losses may be liable to compensate Tiverton Academy for the loss.

If the device has a usage tariff, it should not be used outside of the United Kingdom. In exceptional circumstances where it is required that the device is to be used abroad, prior permission must be sought from the Head Teacher and costs must be kept to a minimum. Mobile data must be turned off when not required. Staff who take a device abroad without such permission and charges are incurred may be liable to compensate Tiverton Academy for the loss.

Premium rate numbers and International numbers must not be called from any device.

3.7 Personal Mobile Phones

Personal mobile phones must not be used at any time in the presence of pupils. Personal mobile phones may only be used during non-contact time and this should be with discretion.

Under no circumstances should personal mobile phones, or other personal electronic equipment, be used to photograph or video pupils.

Only school-owned phones issued by Tiverton Academy are to be visible around school.

3.8 Software

Only software purchased and/or approved by the Senior Leadership may be used on school hardware. Non-standard or unauthorised software can cause problems with the stability of school computing hardware and it is necessary to contact the ICT Leader before the installation of such software. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to.

It is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above or not approved by Senior Leadership must contact the ICT Leader who will be happy to assist in resolving any issues.

3.9 Data Security

You must only access information held on Tiverton Academy's computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

Third party requests for access or sharing of personal or confidential data must be approved by the Head Teacher prior to the third party viewing or being given the requested data.

Personal or confidential data required to be sent to a third party must be protected appropriately, i.e. a list of pupil's name and addresses must not be sent in plain text via an email. Encryption must be used. The 'key' or password required to unencrypt the data must be shared by another communication method, i.e. a telephone call or SMS message to a verified number.

Emailing of encrypted personal or confidential data may only be transmitted to official work email addresses, i.e. @tiverton.bham.sch.uk this includes emails to third parties or other staff members and not personal or free email accounts, such as Hotmail, Gmail or Yahoo.

Personal cloud based storage accounts, such as Dropbox, Google Docs, Microsoft OneDrive etc should not be used to store personal or confidential data.

Storage of personal or sensitive data on a removable device, such as a memory stick, must be encrypted and backed up.

It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up.

3.10 Personal Data and the Data Protection Act

Tiverton Academy maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the Agency's holding and processing of personal data.

It is the responsibility of all Tiverton Academy staff to ensure that personal data is held and processed within the terms of Tiverton Academy's notification and in compliance with the data protection principles.

Personal data shall be:

- obtained processed fairly and lawfully
- held for specified lawful purpose(s)
- not used or disclosed in a way incompatible with the purpose(s)
- adequate, relevant and not excessive for the purpose(s)
- accurate and up to date
- not kept longer than necessary
- available to the data subject
- kept secure.

Tiverton Academy should note that all data and correspondence, including e-mail messages, held by Tiverton Academy may be provided to a data subject, internal or external, in the event of a subject access request.

3.11 Freedom of Information Act

Tiverton Academy is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities. While Tiverton Academy is in the process of meeting the requirements of the Act, employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Therefore, such data or correspondence may be provided to an applicant in the event of an access request once the Act has come into force.

3.12 Virus Protection

Anti-virus software is loaded on all computers as standard and is updated regularly via the network and remotely via the internet. Anti-virus software must not be de-installed or deactivated. Files received by or sent by e-mail are checked for viruses automatically. Users must not intentionally access or transmit computer viruses or similar software.

Non-Tiverton Academy software, hardware or data files intended to be run on school equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer, power off the computer and contact the ICT Leader immediately.

3.13 Network Access

Passwords protect Tiverton Academy systems from access by unauthorised people: they protect your work and the school's information. Therefore never give your network password to anyone else.

Tiverton Academy does not allow the connection of non-school computer equipment to the network without prior request and technical approval. This includes connection via Wi-Fi, dialup or Virtual Private Networking (VPN).

3.14 Further General Guidance

Tiverton Academy users must ensure prior approval at Head teacher level to:

- Set-up World Wide Web sites on Tiverton Academy computing facilities
- Publish pages on external World Wide Web sites containing information relating to Tiverton Academy
- Enter into agreements on behalf of themselves or Tiverton Academy via a network or electronic system
- Be used for external business interests or personal gain

4. Electronic mail

4.1 Use and Responsibility

Tiverton Academy's electronic mail (e-mail) system is provided for the school's purposes. E-mail is now a critical business tool but inappropriate use can expose Tiverton Academy and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

The e-mail system costs the organisation time and money and it must be used judiciously in the same manner as other organisational resources such as telephones and photocopying.

School-wide e-mail messages must be business related and of significant importance to all staff.

4.2 Content

E-mail messages must be treated like any other formal written communication.

E-mail messages cannot be considered to be private, secure or temporary.

Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

Improper statements in e-mail can give rise to personal liability and liability for Tiverton Academy and can constitute a serious disciplinary matter. E-mails that embarrass, misrepresent or convey an unjust or unfavourable impression of Tiverton Academy or its affairs, employees, suppliers, pupils are not permitted. Do not create or send e-mail messages that are defamatory. Defamatory e-mails whether internal or external can constitute a published libel and are actionable. Never send confidential or sensitive information via e-mail. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings.

Do not create or send e-mail messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.

It is never permissible to subject another employee to public humiliation or ridicule; this is equally true via e-mail.

Copyright law applies to e-mail. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 Privacy

E-mail messages to or from you cannot be considered to be private or confidential. Although it is not policy to routinely examine the content of individuals e-mail, Tiverton Academy reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or some legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee wrongdoing, protect the rights or property of the school, and protect ICT system security, identify technical issues or to comply with legal process.

Messages sent or received may be copied and disclosed by Tiverton Academy for lawful purposes without prior notice.

5. Internet usage

The laws of all nation states regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax apply equally to on-line activities. However, the practical legal position regarding Internet usage is often uncertain.

Strictly, documents must not be published on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

Strictly, material must not be accessed from the web which would be objectionable on the above grounds under the sovereign law of the countries in which the networks transporting the material are sited or which would violate the Acceptable Use Policies of those networks.

Given the impracticality of assessing the exact legal position with regard to the previous two paragraphs, Tiverton Academy Acceptable Use Policy governing material that could be objectionable on the above grounds is grounded in English law, on which basis it is reasonable to expect Tiverton Academy employees to have good awareness and to be able to exercise good judgement. If in doubt over a specific case, please refer to the Head teacher or ICT Leader.

Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

All Internet usage from the Tiverton Academy network is monitored and logged. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant employees user account. Such an investigation may result in action via Tiverton Academy's Disciplinary Procedure and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Files so protected must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

5.1 Newsgroups

Postings to newsgroups are in effect e-mails published to the world at large and are subject to the same regulations governing email as above.

Always include a disclaimer with a posting if it could be interpreted as an official statement or policy of Tiverton Academy. For example:

"The views expressed are my own and do not necessarily represent the views or policy of my employer."

5.2 Instant Messaging

Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, Tiverton Academy does not currently allow the use of instant messaging for the communication of sensitive or proprietary Agency information.

5.3 Social Networking and Social Media

The access of Social Networking sites from any computer or mobile device at Tiverton Academy is forbidden.

6. Private use, legislation and disciplinary procedures

6.1 Private Use

Computing facilities are provided for Tiverton Academy's school purposes and responsible personal use is allowed provided there is no conflict with the interests or requirements of Tiverton Academy. Tiverton Academy does not accept liability for any personal loss or damage incurred through using the school computing facilities for private use.

Although Tiverton Academy respect your privacy, any private usage will still be logged and data maybe recorded whether on or offsite. It may be viewed by Senior Leadership or technical staff. It is advisable that if you do not wish such data to be seen that you do not carry out the activity on a school owned device.

6.2 Updates to this Policy

In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification of any updates will be made to all Tiverton Academy network users via their official school email address or in writing.

6.3 Relevant Legislation

The following are a list of Acts that apply to the use of Tiverton Academy computing facilities:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

6.5 Disciplinary and Related Action

Tiverton Academy wishes to promote the highest standards in relation to good practice and security in the use of information technology. All pupils, staff, governors, visitors and supply staff agree to uphold the provisions of this policy. Non-compliance may result in loss of access to the school system, referral to staff disciplinary procedures. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Appendix A:

Examples of behaviours which require the use of Tiverton Academy's disciplinary procedures

GROSS MISCONDUCT Examples

1. Criminal Acts – for example in relation to child pornography
2. Visiting pornographic sites (adult top shelf materials) except where this forms an authorised part of the employees job (for example 'testing').
3. Harassment – inappropriate e-mails or printed e-mails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace.
4. Obscene racist jokes or remarks which have been shared internally and externally – reflects on the image of employer and brings the organisation into disrepute
5. Downloading and installation of unlicensed products
6. Viewing sexually explicit materials, except where this forms an authorised part of the employee's job (for example 'Gridwatch').
7. Chat rooms – sexual discourse, arrangements for sexual activity

MISCONDUCT Examples

8. Frivolous use of Company computing facilities that risk bringing Tiverton Academy into disrepute. The distribution of animated Christmas card programmes or 'chain e-mails' beyond the internal e-mail system would represent examples of such misconduct.
9. Entering into contracts via the Internet that misrepresents Tiverton Academy. Contracts are legally binding agreements and an employee must not enter into any agreements via the Internet to procure goods or services where Tiverton Academy is liable for this contract, without first consulting Tiverton Academy's financial procedures.
10. Deliberate introduction of viruses to systems

This list is not exhaustive, but sets the framework of Tiverton Academy's approach to misuse of computing systems.

Tiverton Academy has the right to monitor employees' use of computer equipment where there is evidence to suggest misuse. (Regulation of Investigatory Powers Act 2000).

Appendix B: Acceptable Use Policy for School Staff

I confirm that I have read and understood the **School's Acceptable Use and E-Safety Policy** and that I will use all means of electronic equipment provided to me by the school and any personal devices which I use whilst at work in accordance with the document. In particular:

- I understand all activity whilst using school owned electronic equipment or accessing services provided by Tiverton Academy may result in all activity being recorded, including the device location and IP address being recorded.
- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school, in accordance with the school's Staff Social Networking Policy.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone where applicable) as contact details for pupils and their parents.
- I will not use my personal mobile phone at any time in the presence of pupils. I understand that I may only use my personal mobile phone during non-contact time and that this should be with discretion.
- I will not use my personal mobile phone, or other personal electronic equipment, to photograph or video pupils.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will take all reasonable steps to ensure that all personal computers, laptops, mobile devices and memory devices are fully virus protected and that protection is kept up to date to reduce the risk of the school network becoming infected.
- I will report any accidental access to material which might be considered unacceptable immediately through the school's e-safety incident reporting system.
- Confidential or Sensitive information which is not stored on the school network will only be stored on a device which is encrypted and a strong password used.
- Computers will be fully logged off or the screen locked before being left unattended. This is especially important when logged in.
- Mobile devices will be either turned off or locked using a pin code before being left unattended.
- I understand that I have the same obligation to protect school data when working on a computer outside school.
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken.

I understand that the school may monitor or check my use of ICT equipment and electronic devices and request to access it at any time.

I understand that by not following these rules I may be subject to the School's disciplinary procedures. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Name.....

Position……...

Signed.....

Date…….

Appendix C:

Acceptable Use Policy for temporary or supply staff and visitors to school

As a visitor to the school I recognise that it is my responsibility to follow school E-Safety procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school.
- I will not use a personal computer I have brought into school for any activity which might be in conflict with my presence in the school.
- I will not take photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned.
- I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to contact pupils unless specific permission is given.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will not use my personal mobile phone at any time in the presence of pupils. I understand that I may only use my personal mobile phone during non-contact time and that this should be with discretion.
- I will not use my personal mobile phone, or other personal electronic equipment, to photograph or video pupils.
- I will report any accidental access to material which might be considered unacceptable immediately through the school's e-safety incident reporting system.
- If I have access to any confidential school information, pupil information or data it will only be removed from the school site with written permission and if so, it will be carried on a device which is encrypted.
- I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken.
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff through the school's e-safety incident reporting system.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school may monitor or check my use of ICT equipment and electronic communications. I understand that by not following these rules I may be subject to the disciplinary procedures.

Name.....

Signed.....

Date……

Appendix D:

Acceptable Use Policy for Primary Pupils in school.

- I will take care of computers and ICT equipment and will not do anything deliberate to break them.
- I will only use the Internet or e-mail when I *am with a teacher, and* have been given permission to do so.
- I will only use the school ICT equipment for purposes I have agreed with a member of staff.
- I will only look at websites that my teacher allows me to.
- I will use the school's search facility (on my Learning Platform) to search for websites and images/pictures on the Internet.
- I will not try to download programmes or files from the Internet.
- I will only print when I have permission from a teacher.
- I will use only my own username and password, unless a teacher tells me to use a different one.
- I will keep my username and password private.
- I understand that I must not bring software or memory sticks/cards into school without permission.
- I will only look at or delete my own files, unless told to by a teacher.
- I understand that I should only publish material on the internet that is my own work
- I know I need permission to take someone's photograph or video them
- Any messages I post on the Learning Platform/internet or send in an email will be polite and responsible
- I will only send e-mails to people that my teacher allows me to.
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I will tell my teacher straight away if I see something on a computer that is wrong, or makes me feel upset or uncomfortable.
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I will tell my teacher straight away if I get a message or an e-mail from someone I have not met or I do not know.
- I understand that the school may check what I am doing, check my computer files and see the Internet sites I visit.
- I understand that the school may talk to my parent or carer if they are worried about my E-Safety

I understand the rules that I must follow for responsible Internet and computer use. I understand that if I do not follow these rules I will receive a suitable punishment immediately and that my computer log in may be turned off for a period of time. This may also apply even if the activity was done outside school.

Pupil name.....

Signed.....

Date.....