# St Mary's C.E.V.C. Primary School
# Online Safety Policy

## Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum (2014) requires pupils to learn how to locate, retrieve and exchange information and create content and code online. In delivering the curriculum, teachers need to plan to integrate the use of technologies such as web-based resources, e-mail and mobile learning. Digital skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill. To deliver this, secure and effective internet access is a necessary entitlement for pupils and an essential resource for staff.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

## 1. Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management of information and administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Children use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

## 2. How will Internet use enhance learning?

- The Internet enables learning anytime, anywhere.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in content creation, communication and research (including the skills of knowledge location, retrieval and evaluation). Furthermore, the computing curriculum (2014) requires pupils to gain an understanding of how the internet works.
- Pupils will learn appropriate Internet use
- Pupils will be given clear objectives for Internet use.

## 3. How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access, i.e. through the Responsible Use agreement for pupils and for staff. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
- Primary pupils' home-school agreement will include the Responsible Use agreement.
- Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
- Where pupils are posting to an online space or webpage (e.g. blogging) as part of their school work, content will be moderated by staff before the posting can be seen online.

# 4. How will filtering be managed?

- The school Internet access will be filtered by the ISP (Internet Service Provider) as appropriate to the age of pupils. The school uses EXA Education's NetASQ Internet Filtering system.
- Ideally inappropriate material would not be visible to children using the web but this is not easy to achieve in all circumstances and cannot be guaranteed by any institution. Children will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
- The Head teacher, Deputy Head teacher, Computing Co-ordinator and ICT technician will manage the permitting and banning of additional web sites identified by the school.
- The school will work in partnership with parents, Wiltshire County Council, DFE and the school's ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (EXA Education) via the Computing Co-ordinator or ICT Technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (IWF - http://www.iwf.org.uk/) by the Head teacher, Deputy Head teacher, Computing Co-ordinator or ICT technician.

# 5. How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school internet enabled device. Neither the school nor Wiltshire County Council can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed annually by the Computing Coordinator.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

# 6. How is online content managed?

- Children will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to EXA Education (the school's ISP).
- Specific lessons will be included within the curriculum to teach all pupils how to develop their media literacy skills (in particular validity and bias). Children will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Where pupils are posting to an online space or webpage (e.g. blogging) as part of their school work, content will be moderated by staff before the posting can be seen online.
- Training is available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

# 7. How should website content be managed?

- Publication of any information online will always be considered from a personal and school security viewpoint.
- The point of contact on the website should be the school address, school e-mail and telephone number.

- Staff or pupils' home information will not be published.
- Written permission from parents or carers will be obtained before photographs/videos of pupils are published on the school website.
- Website photographs/videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Where audio and video are included (e.g. podcasts and video blogs) the nature of the items uploaded will not include content that allows the pupils to be identified.
- The Headteacher (or nominee) will take overall editorial responsibility and ensure that content is accurate and appropriate.

# 8. How are e-mail and digital messaging managed?

- Pupils may only use approved e-mail and messaging accounts on the school system. Access in school to external personal e-mail and messaging accounts is not allowed.
- Pupils must immediately tell a teacher if they receive offensive e-mails or messages.
- Pupils must not reveal details of themselves or others in e-mail or messaging communications, such as address or telephone number, or arrange to meet anyone.
- Whole-class or group e-mail addresses should be used.
- Pupils should use email and messaging in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school behaviour policies and will be dealt with accordingly.
- E-mail or messages sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

# 9. Can mobile phones be brought into school?

- The school's mobile devices provide the primary way pupils access the internet and so devices from home should not be brought into school.
- Children are not permitted to use personal mobile phones within the school (except in exceptional circumstances).
- If a phone is brought into school, pupils will be asked to give them to their teacher or reception staff at the start of the school day. However, they remain the responsibility of the user and the school accepts no responsibility for the loss, theft or damage of such items.
- Children must not take mobile phones on school trips.
- School staff, as authorised by the Head teacher, may search children or their possessions, and confiscate any mobile device they believe is being used to contravene school policy or is considered harmful or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.

# 10 How will we assess emerging technologies?

- Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, video conferencing, Internet access, collaboration and multimedia tools. A risk assessment will be completed on each new technology and assessed for effective and safe practice in classroom use before use in school is allowed. The risk assessment will be evaluated by a member of the Senior Leadership Team (SLT).

# 11 How will we teach children about cyber-bullying?

- Many children and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that children, school staff and parents/carers understand how cyber-bullying is different from other forms of bullying. It is important to understand how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety within our school.

- Cyber bullying can be defined as *"the use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone"* DCSF 2007. The DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyber-bullying: http://www.digizen.org/cyberbullying.
- Cyber-bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Anti-bullying and Child Protection policies.
- In order to identify the bully, the school will undertake all appropriate steps. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

## 11.1 Children using on-line communications and social networking

- The school will conduct regular pupil surveys about home use of digital technologies. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- The use of online chat is not permitted in school, other than as part of a learning task. It must only take place between school-owned devices connected within the school's network.
- Children will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Children must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or arrange to meet anyone.
- Children will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Children will be taught responsible personal publishing through age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Children will be taught the importance of approving and inviting only known friends and to deny access to others by making profiles private. They will be taught how to block and report all unwanted communications.
- Concerns regarding children's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning children's underage use of sites. This will include access to materials viewed via DVD or video games, as well as online.

## 11.2 Parents/carers using on-line communications and social networking

- Parents'/carers' attention will be drawn to the school Internet Safety policy in newsletters and on the school Website
- Information will be provided to parents/carers about how to ensure they can work with the school to ensure social networking is used appropriately both at home by parents/carers and their children.
- A partnership approach with parents/carers will be encouraged. This could include parent's evening, school newsletter, e-safety training with suggestions for safe Internet use at home.
- Interested parents/carers will be referred to organisations such as Childnet International, PIN, Parents Online and NCH Action for Children.
- Parents wishing to photograph or video at an event, either in school or off-site at a school related event, must not post images captured to the Internet, in compliance with the school's policy.
- Parents are asked to carefully consider, before posting content on social media sites, whether it is appropriate to post certain content or if to do so would bring the school into disrepute, breach confidentiality or copyright or if it could be considered offensive, defamatory, discriminatory, bullying or is potential harassment to an individual employed by the school. Where incidents of this nature are brought to the attention of the Senior Leadership Team, and they are deemed to be defamatory in some way, parents will be invited into school to discuss the matter further and the school may request the removal of the post, or where necessary report abuse to the site involved or other authorities.

## 11.3 Staff's professional use of online communications and social networking

- All staff including teachers, supply staff, classroom assistants and support staff, will be asked to sign the policy for responsible e-mail, network and Internet use (see appendix below).
- The school's consequences for Internet and mobile phone/ technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff official blogs kept for educational purposes will be password protected and only operate with approval from the SLT.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and must be used in a safe and professional way as outlined in this policy. This includes expectations around the personal use of social media outside of school (see 11.4)
- In line with *'Guidance for Safer Working Practice for Adults who Work with Children and Young People'* it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers, using personal e-mails addresses. Express care is also to be taken regarding the use of social networking sites.
- Community users of the school's network, devices and online facilities must sign the acceptable user policy before being granted access.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.
- Employees may make occasional and reasonable personal use of the internet (during lunch and break times), as long as this does not interfere with the performance of their duties or the work of other colleagues.
- Employees' access of social media for personal use on their own equipment (e.g. mobile phone, smartphone etc.) is only acceptable during official breaks.

## 11.4 Staff (and volunteers) personal use of online communications and social networking

- Many employees make use of social media in a personal capacity and this policy is not intended to limit their use or enjoyment of social media. However employees should remember that, even when not acting on the school's behalf, they can be held accountable for content which they post on social media sites which could be potentially damaging to the school.
- Damaging content includes any communication made in a personal capacity through social media which:
    - Brings the school into disrepute (e.g. criticising the school, pupils/students or colleagues/governors in an inappropriate manner, posting images that are inappropriate or links to inappropriate content).
    - Breaches confidentiality (e.g. revealing information owned by the school; giving away confidential information about an individual (such as a colleague or pupil/student) or discussing the school's internal workings, such as school budget spending that has not been communicated to the public).
    - Is discriminatory against, or bullying or harassment of, any group or individual (e.g. making offensive or derogatory comments relating to sex, gender reassignment, race (including ethnicity), disability, sexual orientation, religion or belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive, or links to such content).
    - Breaches copyright (e.g. by using someone else's images or written content without permission).
- Employees must consider who can read what is posted, they must be aware that some sites are open to all and other sites allow the employee to control who can see what has been posted.

- Employees need to ensure that they have reviewed privacy settings so that only those who they wish to read the content are able to do so.
- Employees should not include their workplace and/or job title on their profile – being aware that this may make it easier for pupils/students, parents and members of the public to contact them in their personal time.

# 12 Introducing the Internet Safety Policy to Pupils

- Online Safety teaching will be included in the curriculum for all pupils and cover safe use at school and home.
- Rules for Internet access will be posted in all rooms where computers are used.
- The school website includes information on Internet Safety page with information for children and parents and links to useful websites.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use and digital communications will be monitored.

# 13. How will complaints be handled?

- The school has a separate Complaints Policy which applies in all cases relating to online safety and misuse and runs alongside this policy. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school.
- A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. More serious issues may require a range of sanctions, linked to the school's behaviour policy.
- All records of the incident and evidence should be kept, e.g. e-mails saved or printed, text messages saved etc.
- Complains of a child protection nature will be dealt with in accordance with the Local Authority's Child Protection procedures.
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher and/or Chair of Governors.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police need to be contacted. Early contact could be made to establish the legal position and discuss strategies.
- The school will not routinely monitor the webpages that an employee can access from their school laptop, however full logs are retained and can be accessed as part of a genuine investigation.
- The school does not monitor employee's personal social media pages. However, as with any allegation of misconduct, the school will investigate where breaches of this policy are brought to its attention by any means (e.g. via members of the public, employees, parents or children). Investigations which involve social media content will take into consideration:
    - the intent of the content;
    - the "moral intensity" of the content – what damage has been done;
    - the implications – including the level of risk it places the school at (including reputation, data, etc.) and management time;
    - the impact – on work colleagues, the public status of the school, morale etc.;
    - the individual's right to freedom of expression (provided it is not discriminatory, damaging, malicious or libellous).

**Appendix 1**

# St Mary's C.E.V.C. Primary School
# Responsible Internet Use

**These rules help us to be fair to others and keep everyone safe.**

- I will ask permission before using the Internet.
- I will keep school login and password information secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only message, e-mail and open attachments from people I know, or that my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my digital files, messages and e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. EXA Education monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

**Appendix 2**

# St Mary's C.E.V.C. Primary School

## Sample Letter to Parents

Date

Dear Parents

**Responsible Internet Use**

As part of your child's curriculum and the development of computing skills, St Mary's C.E.V.C. Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and digital communication is a worthwhile and essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, (EXA Education) operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

In the hope that you may continue your own safe practice using the internet as a family at home we have included some websites for your use. If you do not have access at home you may wish to use facilities at your local library.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Mrs N Clarke
Headteacher

**Appendix 3**

# St Mary's C.E.V.C. Primary School's Responsible Internet Use Agreement

Please complete, sign and return to the school

| **Pupil:** | **Class:** |
|---|---|

**Pupil's Agreement**

I have read and I understand the school rules for Responsible Internet Use. I will use the school's digital devices and Internet in a responsible way and follow these rules at all times.

| **Signed:** | **Date:** |
|---|---|

**Parent's Consent for Internet Access**

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

| **Signed:** | **Date:** |
|---|---|

**Parent's Consent for Web Publication of Work and Photographs**

I agree that, if selected, my son/daughter's work may be published on the school Website. I also agree that images, sound files and video that include my son/daughter may be published subject to the school rules that this content will not clearly identify individuals and that full names will not be used.

| **Signed:** | **Date:** |
|---|---|

**Parental Agreement to Considerate Use of Social Media**

I will ensure social networking is used appropriately by adults and our children at home. I understand that it is illegal for most social networking sites to be accessed by children under 13 years old.

I understand that photographs or videos taken at an event, either in school or off-site at a school related event, must not be posted to the Internet without express permission of the school and the parents of all children shown in any image. I understand this extends to other family members/guests attending school events.

Before posting comments on social media sites, I will always carefully consider whether it is appropriate or if to do so would bring the school into disrepute, breach confidentiality or copyright or if it could be considered offensive, defamatory, discriminatory, bullying or potential harassment to an individual employed by the school. (I understand that in such circumstances, action will be taken by the school and its representatives to deal with messages and postings deemed to be defamatory and appropriate authorities will be involved).

| **Signed:** | **Date:** |
|---|---|
| **Print name:** | |

**Appendix 4**

## Parental consent form for use of children's media

At St Mary's C.E.V.C. Primary School we take the issue of child safety very seriously, and this includes the use of images, sound files and video of children.

Including images of children in school publications and on the school website can be motivating for the children involved, and provide a good opportunity to promote the work of the school. However, schools have a duty of care towards children, which means that children must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents consent to the school taking and using photographs and images of their children. Any use of children's images at St Mary's C.E.V.C. Primary School is underpinned by our Online Safety policy. We will never include the full name of the child alongside an image.

Please complete, sign and return this form to the school office

---.

I consent to photographs and digital media of the child named below, appearing in St Mary's C.E.V.C. Primary School printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media to promote the activities of the school.

**Name of child:** .....

**Name of parent or guardian:** .....

**Address:** .....

.....

.....

**Signature:** .....

**Date:**.....

**Appendix 5**

## Digital Agreement for St Mary's C.E.V.C. Primary School Staff

### 1. Digital devices

2. Digital devices (e.g. a laptop or iPad) remain the property of St Mary's C.E.V.C. Primary School.
3. The device is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only St Mary's C.E.V.C. Primary School Staff or Supply Teachers should use the device.
4. On the teacher leaving the school's employment, the device is returned to St Mary's C.E.V.C. Primary School. Staff on extended leave of 4 weeks and over should return their devices to the school (other than by prior agreement with the Headteacher).
5. When in school and not being used, the device must be switched off and kept secure. (N.B. Pressing **+ L** will lock a Windows laptop).
6. Whenever possible, the device must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
7. The device must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher with evidence of adequate insurance.
8. Staff may ask the ICT Technician to load their own software onto a device, but it must be fully licensed and not corrupt any software or systems already installed on the device.
9. Any software loaded must not affect the integrity of the school network.
10. If any removable media is used then it must be checked to ensure it is free from any viruses.
11. It will be the responsibility of the ICT Technician to ensure virus protection software that has been installed on the laptop is kept up to date.
12. Staff must use their device in school on the network at least once a week to ensure virus protection is automatically updated.
13. Staff should not attempt to significantly alter the device settings other than to personalise their desktop working area.
14. If any fault occurs with the device, it should be referred immediately to the ICT Technician.
15. When being transported, the carrying case supplied must be used at all times.
16. The device would be covered by normal household insurance. If not it should be kept in school and locked up overnight.
17. Staff must take responsibility for ensuring that data storage devices are kept safe and secure at all times.

## 2. Responsible e-mail, messaging network and Internet use

1. I will use all digital equipment issued to me in an appropriate way. I will not:
   - Access offensive website or download offensive material.
   - Make excessive personal use of the Internet or e-mail.
   - Copy information from the Internet that is copyright or without the owner's permission.
   - Place inappropriate material onto the Internet.
   - Will not send e-mails that are offensive or otherwise inappropriate.
   - Disregard my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the device and school network.
   - Access the files of others or attempt to alter the device settings.
   - Update web pages etc. or use pictures or text that can identify the school, without the permission of the Headteacher.
   - Attempt to repair or interfere with the components, software or peripherals of any device that is the property of St Mary's C.E.V.C. Primary School.
2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the school's ICT Technician as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working.
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the Headteacher and register the passwords with the Headteacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager.
9. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
10. I will report immediately to the Headteacher any unpleasant material or messages sent to me.
11. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
12. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
13. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.

14. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
15. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

**Name**.....

**Signature:**.....

**Date:** .....