ENGAGE
ENLIGHTEN
EMPOWER

Educore Services
PO Box 110506
Solwezi, Zambia
Telephone: +260 963 89 85 52
enquiry@educoreservices.com
www.educoreservices.com

E-Safety Policy

Table of Contents

Publication Date	October 2018
Review Date	October 2020
Next Review Date	October 2022
School Leader Responsible	Head/SLT
Senior Management Responsible	CEO

1. Rationale

All Educore Services schools understand the integral part electronic connection has to play in learning about the modern world. The opportunities for learning created by providing access to such a world are limitless, and must therefore be part of day to day teaching and learning. Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, and 'cyber' bullying and identity theft. It must therefore be the role of each of our schools to ensure that such risks are minimised, and, more importantly, that children and young people are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy on-line citizens.

2. Aims and Objectives

This policy offers guidelines on safe use of electronics and internet-connected devices and outlines responsibilities and procedures which are in place to keep our students as technologically educated and safe online as possible.

3. Responsibilities of Stakeholders

We believe that e-safety is the responsibility of the whole Educore community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community should contribute to e-safety:

3.1 Responsibilities of each school's leadership team

- Develop and promote an e-safety culture within their school community.
- Read, understand and adhere to any requirements or information given to them by the IT Manager and IT HoD on best practice, guidance and legislation.

- Support the IT Manager and their ICT teachers in their work.
- Make appropriate resources, training and support available to members of their school community to ensure they are able to carry out their roles with regard to e-safety effectively, including making them aware of procedures to be followed should an e-safety incident occur in their school.
- Receive and regularly review e-safety incident logs, share these with the IT Manager where necessary (should the incident have a bearing on wider group policies or practices, or on group-wide IT systems and processes), and be aware of the procedure to be followed should an e-safety incident occur in their school.
- Support their pupils and their families so they are able to adhere to their own IT responsibilities as laid out in section 3.5 and 3.6 below, including ensuring they have the tools and learning to do so.

3.2 Responsibilities of each school's lead IT teacher or Head of IT

- Promote an awareness and commitment to e-safety throughout the school.
- Read, understand and adhere to any information or requirements given to them by the IT Manager, as well as keeping abreast of current guidance, legislation and best practice on e-safety and technology use.
- Create and maintain any necessary school-specific e-safety procedures, and ensure that the IT Manager is aware of individual school processes.
- Maintain an understanding of current e-safety issues, guidance and appropriate legislation, and ensure these are communicated to their senior leadership team. Maintain a good channel of communication with the IT Manager in this regard also.
- Ensure all members of staff at their school receive an appropriate level of training in e-safety issues and that this is regularly updated.
- Ensure that e-safety education is embedded across the curriculum in their school, and students know how to keep themselves safe online and what to do if they do not feel safe or if they think an incident has occured.
- Ensure that e-safety is promoted to parents and carers and information about how to keep their children safe online is clearly stated in uncomplicated language, and readily available to the parent community.
- Model safe and responsible behaviours in their own technology use and maintain a professional level of conduct in their personal use of technology at all times.
- Monitor and report on e-safety issues to their senior leadership team as appropriate and ensure the e-safety incident log is kept up-to-date.
- Support their pupils and their families so they are able to adhere to their own IT responsibilities as laid out in sections 3.5 and 3.6 below, including ensuring they have the tools and learning to do so.

3.3 Responsibilities of Teachers and Support Staff

- Read, understand and help promote group-wide and school-specific e-safety policies and guidance.
- Develop and maintain an awareness of current e-safety issues and guidance as guided by their own understanding and information given to them by their IT colleagues.
- Model safe and responsible behaviours in their own use of technology and maintain a professional level of conduct in their personal use of technology at all times.
- Embed e-safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology and ensure any school-specific procedures are followed.
- Be aware of what to do if an e-safety incident occurs.
- Support their pupils so they are able to adhere to their own IT responsibilities as laid out in section 3.5 below.

3.4 Responsibilities of Technical Staff

- Support each school in providing a safe technical infrastructure to support learning and teaching as shaped by their specific demographic, context and budget.
- Take responsibility for the security of both school and central IT systems. • Report any e-safety-related issues that come to your attention to the relevant school leadership teams and IT teaching staff.
- Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to your work.

- Maintain a professional level of conduct in their personal use of technology at all times.
- Read, understand, contribute to and help promote the school's e-safety policies and guidance. • Read, understand and adhere to the Acceptable Use Policy (AUP).
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school Computing infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.

3.5 Responsibilities of Pupils

- Understand and adhere to their school's rules and codes of conduct around using computer or phone technology in school, with the guidance from their teachers.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies in school and at home.
- Take responsibility for their own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what actions they should take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if they know of someone who this is happening to.
- Discuss e-safety issues with family and friends in an open and honest way.

3.6 Responsibilities of Parents and Carers

- Help and support their school in promoting e-safety.
- Read, understand and promote any school policies or other information about IT use with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with their school if they have any concerns about their children's use of technology.

4. Teaching & Learning

Educore Services teachers know that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school communities, lies in effective education. At Educore we know that the internet and other technologies are embedded in children's lives both in and outside school, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

Activities schools can commit to to promote safe and responsible online behaviours include but are not limited to:

- Providing a series of specific e-safety-related lessons in every year group/specific year groups as part of the IT or Computing curriculum / other lessons.
- Celebrating and promoting e-safety through assemblies and whole-school activities, including promoting a Safer Internet Day each year.
- Discussing, reminding or raising relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Reminding pupils about their responsibilities through an end-user AUP which every pupil will accept when they log on.

- Staff modelling safe and responsible behaviour in their own use of technology both during and outside lessons.

5. Parent/Carer Engagement

It is important to help all our parents at all our schools develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.
Activities individual schools can commit to which will help our parents in this area include but are not limited to:

- Holding parent workshops on e-safety
- Including useful links and advice on e-safety in school newsletters.

6. IT and Internet Monitoring & Usage

6.1 Managing IT Systems

- Educore Services central IT will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up- to-date.
- Educore Services IT and individual school leadership will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- All users, whether student or staff, will accept an end-user Acceptable Use Policy (AUP) provided by Educore Services IT department, appropriate to their age and access.
- Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, any Educore Services IT systems, and that such activity will be monitored and checked by theit IT HoD and the IT Manager.
- In all primary phases, Internet access using school computers will be supervised at all times by a member of staff. In secondary, Internet access will be supervised either remotely or in person.
- In some schools, once an AUP form has been signed, individual student devices are granted access to the school server.
- Members of staff will access the Internet on their school or registered personal devices. Access to Windows on school devices is through an individual log on. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school IT systems should be kept secure and available to at least two members of staff, e.g. the Head of Department for IT and a member of the senior leadership team at that school.
- The wireless network in school is encrypted to reduce the risk of unauthorised access.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material, although it is not possible to guarantee that access to unsuitable material will never occur.
- Educore Services central IT will regularly audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. This policy will be reviewed and updated biannually. We will regularly review all schools' internet access provision, and review new methods to identify, assess and minimise risks.

6.2 Filtering the Internet

All schools use a filtered Internet service. The filtering is provided through PF-Sense.

If users discover a website with inappropriate content, this should be reported to a member of staff who will inform their IT lead teacher and/or the IT Manager. If users discover a website with potentially illegal content, this should be reported immediately to the IT Manager. Educore Services will report this to appropriate agencies including the filtering provider.

Educore Services will regularly review the filtering and other security systems to ensure they meet the needs of all users.

6.3 Use of Learning Technologies in Schools

Each school has a variety of learning technologies to enhance teaching and learning. Below outlines their use and the use of devices brought into each school during normal face to face learning. This list may change during any periods of remote learning, for example schools may communicate with their students through instant messaging, video conferencing, and mobile phones.

	TCS		TPS		TPK		SKAB		SKAL		FNK	
	Pupils	Staff	Pupils	Staff	Pupils	Staff	Pupils	Staff	Pupils	Staff	Pupils	Staff
Personal mobile phones brought into school	Yes	Yes	No	Yes	No	Yes	Boarders with individual permission	Yes	No	Yes	No	Yes
Mobile phones used in lessons	No	No (except with individual permission ie Matrons)	No	No	No	No	No	No	No	No	No	No
Mobile phones used outside of lessons	Boarders	Yes	No	Yes	No	Yes	Boarders with individual permission	Yes	No	Yes	No	Yes
Taking photos or videos on personal equipment	Yes	No *as per guidelines of photo permission form	no	No	No	No	Yes	No	No	No	No	No
Taking photos or videos on school devices	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Use of personal email addresses in school	No	No	No	No	No	No	No	No	No	No	No	No
Use of school email addresses for personal correspondence	No	No	No	No	No	No	No	No	No	No	No	No
Use of online chat rooms	No	No	No	No	No	No	No	No	No	No	No	No
Use of instant messaging services (specifically in times of remote learning) limited to those ratified by the school	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Use of blogs, wikis, podcasts or social networking sites for communication with school community	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Use of video conferencing/online video meetings	Yes	yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

6.4 Using Email

- Staff should use the Educore Services approved email account allocated to them by the company, and be aware that their use of this email system will be monitored and checked.
- Pupils will be allocated personal email addresses only with authorisation from the school head.

- Communication between staff and the wider school community should be professional.
- Any inappropriate use of the Educore Services email system, or the receipt of any inappropriate messages by a user, should be reported to a member of the central IT department.

6.5 Using Media

All students need to be reminded by their teachers of safe and responsible behaviours when creating, using and storing digital images, video and sound. Teachers must remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

- Digital images, video and sound will be created using equipment provided by the school or authorised by the school Head.
- Staff will follow safeguarding policy on creating, using and storing digital resources. Specifically, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved. If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Nothing containing school branding, images or insignia should be shared publicly on any platform by either students or staff without the express permission of the school Head.

6.6 Virtual Learning Environments and Social Networking

Our schools use a number of virtual learning environments to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Pupils will model safe and responsible behaviour in their creation and publishing of online content within their individual school's learning platform.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

6.7 New Technologies

As an organisation we will keep abreast of new technologies and consider both the benefits of these for learning and teaching and also their risks from an e-safety point of view. We will regularly amend the e-safety policy to reflect any new technology that has been introduced to any of our schools or other departments, or to reflect the use of new technology by pupils which may cause an e-safety risk.

7. Protecting Personal Data

Educore Services ensures that personal data is recorded, processed, transferred and made available according to the 2018 Zambian Data Protection Bill.

- All staff will ensure they properly log-off from a computer terminal after accessing personal data.
- All staff will ensure they properly log-out from ISAMS and other pupil data systems after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of their school leadership team. Any data which is impractical to ensure is kept in school will be kept secure, by use of Educore Services laptops which are password protected or on an USB Flash drive.

8. School Websites

- No Educore Services school or company website will include the personal details, including personal email addresses, of staff or pupils. School email addresses are included on some school websites to enable prent-teacher communication. A generic contact e-mail address will be used for all other enquiries received through the school websites.

- All content included on any Educore Services school or company website will be approved by that school's Head Teacher, or the relevant department manager before publication.The content of the website will be composed in such a way that individual pupils are not named and identified.
- Staff and pupils should never post school-related content on any external website or social media platform without seeking permission first.

9. Extremism & Radicalisation

The use of social media to engage children and young people with extreme and radical views has changed traditional notions of how terrorist groups communicate, leading to children and young people being exposed to extremist content in the online world. Although this is a low risk in our geographical location, IT systems will ensure children are safe from terrorist and extremist material when accessing the internet in school by establishing appropriate levels of internet filtering.

10. Dealing with E-Safety Incidents

The correct procedure for dealing with e-safety incidents follows the same procedure as dealing with safeguarding incidents, as outlined in the Educore Safeguarding and Child Protection Policy. It is of paramount importance that a member of that school's leadership team, the IT HoD, the school Head Teacher or the Educore Services IT Manager is made aware of any e-safety incidents immediately and the case is documented. The student's parents\house parent are to be notifed of the event especially if the child is in immediate danger.

11. Virtual Learning Periods

In times of necessary school closure (for example, during a pandemic), students may be supported by the school to continue their learning at home. This type of support will vary across the Educore group according to age group, curriculum, and school. Wherever appropriate virtual learning will be offered through the online platforms and resources most suited to that group of students. Expectations and guidelines to ensure consistency are as follows: each school will then devolve their own virtual learning processes from these:

Staff Responsibilities:

When providing remote learning, **teachers** must be available during their normal working hours. If they're unable to work for any reason during this time, for example due to sickness or caring for a dependent, they should report this using the normal absence procedure as outlined in the Educore Short Staff Absence Policy. When providing remote learning, teachers are responsible for:

- Setting work – enough work to cover the period for their own classes and cover for other classes if they have been asked to do so by their HoD. This work needs to be set by 3pm the day before. The work will be uploaded or disseminated on whichever platform the school is using for remote learning. The work set should take into account students who have limited access to devices, and ensure consistency across the year and subject.
- Providing feedback on work – including a clearly communicated plan and deadline to access completed pupil work and share feedback with pupils.
- Keeping in touch with pupils who aren't in school and their parents – complying with individual school expectations on regularity and means of communication with pupils and parents, as well as handling complaints or concerns shared by parents and pupils and handling behavioural and engagement issues. Teachers should know who to liaise with on their staff in the case of complaints or safeguarding concerns.
- Attending virtual meetings with staff, parents and pupils. Whenever meeting virtually with any member of the school community, staff should ensure that they are following school expectations regarding online etiquette (camera/microphone on or off at which points; being in a professional looking location for lessons and meetings – no unmade beds or inappropriate items in the background. Avoiding areas with background noise or avoidable interruptions, public spaces, wearing professional dress even when working from home).

- There may be occasions where staff members are required to teach both face-to-face and remote learning. Individual schools are responsible for letting teachers know their expectations, timetables and resources in this case.

Alongside their teaching responsibilities, **subject leads and other middle leaders** should: consider what aspects of the subject curriculum need to change to accommodate remote learning; work with their departments remotely to make sure work set is consistent and appropriate; work with other middle leaders to ensure deadlines are staggered appropriately; monitor work set and feedback given by their departments according to an agreed monitoring framework, and share resources and ideas with their department to improve the quality of remote learning.

Alongside any teaching responsibilities, **senior leaders** should: coordinate the remote learning approach across the school; monitor the effectiveness of remote learning both quantitatively and qualitatively according to parameters communicated clearly to all staff; organise and lead relevant staff, parent and student meetings, and liaise with the IT department to monitor and ensure the safety of online systems including data protection and safeguarding considerations.

The role of the **Designated Safeguarding Lead (DSL)** in each school is equally important during times of remote learning. Each Educore school has its own specific processes, but in general the DSL in each school should make efforts to be aware of and communicate to relevant staff those children who may be at risk while learning remotely, and to communicate regularly with families considered in need of additional support or at risk of harm. The DSL should be aware of how changes to the mode of learning can affect families, and should communicate clearly to staff, parents and students what steps should be taken if a safeguarding concern is detected.

IT staff are responsible for: fixing system issues, helping staff and parents with technical issues and accessing the internet or devices, reviewing the security of remote learning systems and flagging data protection breaches, and supporting the DSL in ensuring all safeguarding filters and monitoring systems are in place and safeguarding information is updated on the website.

Students can be expected to: be contactable at agreed times during the school day, including committing to being in front of their device and attending lessons at required times; complete work to the deadlines set by their teachers; seek help when they need it; alert teachers in good time if they are not able to complete their work so teachers can support them.

Parents and carers of children working remotely can be expected to: make the school aware if their child is sick or otherwise can't complete work or attend remote learning; seek help from the school if they need it; be respectful and use the appropriate channels when making complaints or concerns known to the school.

Data protection:

Staff members may need to collect and/or share personal data such as email addresses and parent/guardian phone numbers as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals won't need to give permission for this to happen. However, staff are reminded to collect and/or share as little personal data as possible online.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Wherever possible, ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing antivirus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates.

12. Related Policies

The following documents are related to the Educore E-Safety Policy:

Pos	Description	Filename / Link
1	E-Safety Incident Log	
2	Health & Safety Policy	
3	Student Code of Conduct	
4	Acceptable Use Policy	
5	Safeguarding and Child Protection Policy	

12. Annex

The following documents are an integral part of the e-Safety Policy:

Pos	Description	Filename / Link
1	Taking steps to stay safe online: a guide for parents and children	
2	Acceptable Use Policy	

Educore Services
PO Box 110506
Solwezi, Zambia
Telephone: +260 963 89 85 52
enquiry@educoreservices.com
www.educoreservices.com

Annex 1: Taking steps to stay safe online: a guide for parents and children

Parents:

1. Explore together: Ask your child to show you their favourite websites and apps and what they do on them. Listen, show interest and encourage them to teach you the basics of the site or app.

2. Chat little and often about online safety: If you're introducing them to new learning websites and apps while school is closed, take the opportunity to talk to them about how to stay safe on these services and in general. Ask if anything ever worries them while they're online. Make sure they know that if they ever feel worried, they can get help by talking to you or another adult they trust.

3. Help your child identify trusted adults who can help them if they are worried: This includes you and other adults at home, as well as adults from wider family, school or other support services who they are able to contact at this time. Encourage them to draw a picture or write a list of their trusted adults.

4. Be non-judgemental: Explain that you would never blame them for anything that might happen online, and you will always give them calm, loving support.

5. Supervise their online activity: Keep the devices your child uses in communal areas of the house such as in the living room or kitchen where an adult is able to supervise. Children of this age should not access the internet unsupervised in private spaces, such as alone in a bedroom or bathroom.

6. Talk about how their online actions affect others: If your child is engaging with others online, remind them to consider how someone else might feel before they post or share something. If they are considering sharing a photo/video of somebody else, they should always ask permission first.

7. Use 'SafeSearch': Most web search engines will have a 'SafeSearch' function, which will allow you to limit the content your child can access whilst online. Look out for the 'Settings' button on your web browser homepage, which is often shaped like a small cog.

8. Parental controls: Use the parental controls available on your home broadband and all internet enabled devices in your home. You can find out more about how to use parental controls by visiting your broadband provider's website.

Children: Be SMART when using computers at school or at home:

S	**Stay Safe:** Don't give out personal information to people and places you do not know.
M	**Don't Meet Up:** Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
A	**Accepting Files:** Accepting emails, files, pictures or text from people you don't know can cause problems.
R	**Reliable?** Check information before you believe it. Is the person or website telling the truth?
T	**Tell Someone:** Tell an adult if someone or something makes you feel worried or uncomfortable.

Educore Services
PO Box 110506
Solwezi, Zambia
Telephone: +260 963 89 85 52
enquiry@educoreservices.com
www.educoreservices.com

Annex 2: Acceptable Use Policy

In order for Educore Schools to be able to continue to make computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the School's teachers and other Staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

I hereby undertake to use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

Unacceptable uses of the School's internet systems:

- Internet chat.
- Tethering and Wi-Fi Hotspotting off the school network.
- Streaming or watching any online videos.
- Downloading or uploading music, videos, series, games, software and applications, pictures, and so on, without written consent from a teacher.
- Use any prohibited software or apps (e.g. torrenting, VPNs, Proxy, and so on).
- Accessing websites that have adult content and are restricted.
- Accessing restricted websites or accessing restricted software (torrent sites, VPNs, Proxy, and so on)
- Accessing internet intensive sites (e.g. Netflix, YouTube, and so on)
- Plagiarism.

Internet Safety

Students are advised that access to the electronic network may include the potential for access to materials, inappropriate for school-aged pupils. Each student must take responsibility for his or her use of the computer network and Internet and stay away from these sites. If a student finds that other students are visiting offensive or harmful sites, he or she should report such use to a member of staff immediately. If a student does accidentally access this type of information, he or she should immediately notify a teacher.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of websites, the interception of email and the deletion of inappropriate materials in circumstances 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 text or imagery which is unauthorised or unlawful.

Help in raising awareness of acceptable and smart use of internet across Educore Schools:
By signing this acknowledgement form, you are agreeing not only to follow the rules in this Policy but are agreeing to report any misuse of the network to the ICT staff. Misuse means any violations of this Policy or any other use that is not included in the Policy but has the effect of harming another or his or her property.

If I see anything, I am unhappy with or I receive messages I do not like, I will inform a teacher or the ICT staff immediately.

I hereby give permission for the school to check my computer files and understand that the school may monitor the Internet sites that I visit.

I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers and that other punishments could apply in term of the code of conduct and disciplinary action may be taken.

Name: _____

Signature: _____

Year: _____

Date: _____