INVICTUS

Education Trust

Online Safety Policy

Approved by Board of Trustees on 27th September 2021

Reviewed September 2021

To be reviewed by August 2024

Revision Number	Date	Amendment	Document Manager	Document Author
00	March 2019		IT	IT
01	September 2021		IT	IT

Policy Formulated in Consultation with:	Trustees/CEO/Headteachers/DSL's

Contents

1. Introduction

1.1 ICT is provided to support and improve the teaching and learning in our Trust as well as ensuring the smooth operation of our school systems.

1.2 This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.

1.3 The policy also provides advice and guidance to our employees on the safe use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time. However, a breach of this policy is likely to result in disciplinary action.

1.5 The Trust aims to:

a) Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

b) Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)

c) Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Scope and Purpose

2.1 This policy applies to all employees, governors, volunteers, visitors and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to your Headteacher, the Network Managers or a senior member of staff.

2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.

2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.

2.5 If you reasonably believe that a colleague has breached this policy, you should report it without delay to your Headteacher or to the Network Managers.

2.6 This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Monitoring

3.1 The contents of our ICT resources and communications systems are our property. Therefore, employees should have no expectation of privacy in any message, files, data, document, facsimile, social media post, blog, conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems. Data stored on our ICT and communications systems must never be copied or transferred to third-party systems or computers without the permission of the Network Managers. Do not use our ICT resources and communications systems for any matter that you wish to be kept private or confidential. This includes personal transactions such as online purchasing or online banking.

3.2 We reserve the right to monitor, intercept and review, without notice, all activities using our ICT resources and communications systems, including, but not limited to, application use, file use, Internet use, social media postings and activities, and electronic communications, to ensure that our rules are being complied with and are being used for legitimate business purposes. As our employee you consent to such monitoring by your acknowledgement of this policy and your continued use of such resources and systems.

3.3 We may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and may delete such copies from time to time without notice. We reserve the right to recover from backups or archives any data or communications that have been deleted.

4. Policy Rules

4.1 In using the Trust's ICT resources, the following rules should be adhered to. For advice and guidance on these rules and how to ensure compliance with them, you should contact the Network Managers.

4.2 The Network and appropriate use of equipment

(a) You may be permitted to adjust some computer settings for comfort and ease of use but these must be adjusted back after use for the next user. Some settings are restricted and the system will inform you of this if you attempt to change them. You must not attempt to circumvent restrictions with the goal of changing these settings.

(b) Computer hardware has been provided for use by employees and students and is positioned in specific areas. If there is a problem with any equipment or you feel it would be better sited in another position to suit your needs, please contact the school ICT Technician. Only the Network Manager/ICT Technicians will be allowed to move, repair or adjust ICT equipment. You must never move, repair, or adjust hardware without permission.

(c) Do not disclose your login username and password to anyone (unless directed to do so by a senior manager for monitoring purposes or as stated in clause 2.4). This includes other staff members.

(d) You are required to change your password in accordance with the login prompts. Ensure that you create appropriate passwords as directed. Do not write passwords down where they could be used by another individual and do not share your password with anybody.

(e) Do not allow anybody – including other staff or students - to access or use your personal log-on rights to any school systems. Other users may not be permitted the same access rights enjoyed by your account, and this could lead to a breach of Data Protection and network security. Allowing such third-party access could put you at risk if your accounts are used.

(f) Before leaving a computer, you must log off the network or lock the computer, checking that the logging off procedure is complete before you leave. If you are leaving a computer for only a short amount of time, you must ensure that the computer is locked.

(g) Ensure projectors linked to the network are switched off when not in use.

(h) Only software provided by the network may be run on the computers. You are not permitted to download or install applications or games from the Internet, or other third-party sources. If you require software to be installed, you must request this from your school ICT Technician.

(i) You must never use any removable storage devices, or memory sticks on Trust computers. Storing data on removable storage devices or memory sticks risks the data being lost, corrupted, or obtained by third parties. The ICT system is configured to restrict access to removable storage devices – you must never attempt to circumvent these restrictions.

(j) Student or Staff data, or any other confidential information should not be stored on a removable storage device and not taken off the premises. If you are accessing the ICT System remotely (via Remote Desktop or other means), you must never copy this information onto a third-party or home computer.

(k) Student or Staff data, or any other confidential information, must never be saved on cloud storage web sites (such as Google Drive, Dropbox, or a personal One Drive account) without the explicit consent of the Network Managers.

4.3 Mobile Devices and Laptop use

The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device including those provided by the Trust. Referred to as mobile device(s):

(a) The Network Managers can refuse access to the Trust network for any device

(b) You must ensure that your mobile device is password protected. This is essential if you are taking the mobile device off of our premises.

(c) You must not leave your mobile device in an unsafe place, for example in your car.

(d) Mobile devices not provided by us must have up to date anti-virus installed before being connected to the network.

(e) You must ensure you have the appropriate permissions and security in place in order to access our network at home.

(f) Mobile devices owned by the Trust must be returned to the Network Managers/ICT Technicians when requested, so that those devices can be kept secure, up to date and free of viruses and malicious software. When a request is made to return equipment, it must be returned it at the earliest possible time.

(g) You may not install any applications or games on any device provided by the Trust. If you require software to be installed, you must ask your school ICT Technician.

(h) You may change some settings on your mobile device (such as volume, or screen brightness). Some settings will be restricted, and you will be advised of this if you attempt to change them. You must never circumvent restrictions with the aim of changing these settings.

(i) If a mobile device provided by the Trust is lost or stolen, this must be reported to your school ICT Technician, or the Network Managers, at the earliest opportunity. If a mobile device has been stolen, you must also inform the police and obtain a crime reference number.

(j) If you damage a mobile device provided by the Trust, you must report this damage to your school ICT Technician, or the Network Managers, at the earliest opportunity. If the damage is accidental in nature then the device will be repaired and returned to you. If a replacement device is immediately available, this may be loaned to you during the period where repairs are taking place. If the damage is through your negligence, we may seek to recover the cost of repairing the device and/or refuse to loan you another device.

4.4 Internet Safety

(a) Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source. Many criminals present themselves as looking genuine, and so you must be absolutely sure before revealing any confidential information. If you are unsure whether a third-party is genuine, please ask your school ICT Technician, or the Network Managers, for assistance.

(b) Never give out personal information about a pupil or another employee over the Internet without being sure that the request is valid and you have the permission to do so.

(c) <u>Always</u> alert the Network Managers if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring and reporting.

(d) <u>Always</u> alert the Network Managers if you receive any messages that make you feel uncomfortable or you think are unsuitable.

(e) <u>Always</u> alert the Network Manager if you receive a suspicious message with links that can be clicked, even where that message appears to be from somebody you know or for a subject you recognise.

(f) The Trust's ICT and communication systems are subject to automatic monitoring, both for security and safeguarding purposes.

a If a safeguarding incident above a pre-defined severity threshold is discovered, the system will automatically inform the appropriate school's Designated Safeguarding Lead of the incident. The details sent to the appropriate person will contain the name of the person the incident concerns, where it occurred, the date and time at which it occurred, the keyword(s) or phrase(s) that triggered the incident, along with one or more screenshots of the incident.

b If a safeguarding incident is reported to a Designated Safeguarding Lead, the incident will be managed according to the Trust’s Safeguarding Policy. School ICT Technicians and the Network Managers will provide whatever data is requested by the Designated Safeguarding Lead as part of this process. This may involve personal communications, e-mails, or files belonging to staff members or students, and may happen without the consent or knowledge of those parties.

c If a safeguarding incident below a pre-defined threshold is discovered, the incident will be recorded for the Designated Safeguarding Lead to review at an appropriate time.

d If a system security incident is discovered, the Network Managers will be informed. The Network Managers will then investigate the incident in detail and reserve the right to access staff or student files, e-mails, or other communications, in order to ascertain the nature of the incident. Mitigation and/or a resolution will then be implemented, which may involve restricting ICT system access to specific staff and/or students until the incident has been fully resolved.

4.5 Internet and Email

(a) The internet and email facilities are provided to support the aims and objective of the Trust. Both should be used with care and responsibility.

(b) Use of the internet at work must not interfere with the efficient running of the Trust. We reserve the right to remove or restrict internet access to any employee at work.

(c) You must only access those services you have been given permission to use.

(d) You are required to check you work emails at least daily unless you are sick or on annual leave. You are not required to check your e-mails outside of working hours, however you may choose to if you wish.

(e) Before sending an email, you should check it carefully and consider whether the content is appropriate. You should treat emails like you would any other form of formal written communication. If you are sending an e-mail to a third party, such as a parent, you must use appropriate formal language.

(f) Although the email system is provided for business purposes we understand that employees may on occasion need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect, or be to the detriment of, you carrying out your role effectively. When sending personal emails from your work email account you should show the same care in terms of content as when sending work-related emails. You should also remember that the Trust’s e-mail system is automatically monitored for inappropriate material, which may at times involve copies of e-mails being taken. If there are personal matters that you do not wish to be subject to this monitoring, you should not use the Trust's e-mail system for this purpose.

(g) The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure, regardless of whether those e-mails have been sent internally or externally.

(h) You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.

(i) If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address but you should alert the Network Managers.

(j) Do not access any sites which may contain inappropriate material or facilities, as described below:

(i) Proxy

(ii) Dating

(iii) Hacking software

(iv) Pornographic content

(v) Malicious content

(vi) Music downloads

(vii) Non-educational games

(viii) Gambling

(k) Do not send malicious or inappropriate pictures of children or young people including students, or any pornographic images through any email facility. If you are involved in these activities the matter may be referred to the police.

(l) Under no circumstances, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials you must inform the Network Managers.

(m) Do not upload or download unauthorised software and attempt to run on a networked computer.

(n) Do not use the computer network to gain unauthorised access to any other computer network.

(o) Do not attempt to spread viruses or other malicious software threats.

(p) Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.

(q) Never open attachments of files if you are unsure of their origin; delete these files or report to the Network Managers.

(r) Do not download, use or upload any material from the internet, unless you have the owner's permission.

(s) Never click a link in an email that is suspicious, even if it appears that it is from somebody you know, or for a subject you recognise. Links with suggestions such as 'click here to view this message', or similar, must never be clicked.

(t) Never enter your network password into a third-party website. Staff should only enter their network password into web sites provided by the Trust. If staff are in any doubt, consult the Network Managers/ICT Technicians. Some malicious third-party web sites are disguised as genuine web sites designed to fool you into thinking that they are something that they are not – you should be aware of this and always critically decide whether or not you should proceed.

(u) Providing your password to a third party, whether deliberately or negligently, presents a safeguarding risk to our students and to other staff members. This will be considered under the disciplinary procedure.

(v) The use of unsanctioned third-party communication systems and services (including but not limited to, WhatsApp, Facebook Messenger, Signal, or Snapchat) must never be used to conduct school or Trust business. These pose a significant safeguarding and data protection risk. You must always use the Trust's internal or sanctioned third-party communications systems (for example, Invictus InTouch, Invictus Meetings, Office 365, or Microsoft Teams) when conducting Trust or school business. Use of unsanctioned third-party systems will be considered under the disciplinary procedure.

4.6 Remote and Virtual Learning

The following rules apply when conducting online learning (where a student and/or staff member is taking part in a lesson or other session remotely) and when conducting online meetings, both with internal attendees and external attendees.

(a) All live virtual lessons must take place using the Trust's approved platform, BigBlueButton. This platform is accessed via the Extra Sessions section of each school's Learning Platform. None-live lessons may take place through sanctioned third-party systems (including but not limited to, MyMaths, Hegarty Learning, or Kahoot)

(b) When conducting a live virtual lesson, staff members may choose whether or not to enable their own webcam. If they choose to do this, they should ensure that they are wearing appropriate attire for the lesson, and that their background is either physically clear of inappropriate content, or the background is blurred. Staff members are expected to use professional discretion as to what is appropriate to be in the background.

(c) Staff members may choose to enable student webcams during a virtual lesson, however students are permitted to decline this. Staff members must never compel or otherwise pressure or coerce students into enabling their webcams if they do not wish to.

(d) Staff members may choose whether to enable their microphones during a virtual lesson. If you choose to enable your microphone, you must ensure that nothing inappropriate is audible to students. If a disruption is unavoidable, you must temporarily disable your microphone.

(e) All activity during a virtual lesson is logged and monitored

(f) Staff members may choose to record a virtual lesson. If they choose to do this, the recording must be kept within the system and may not be exported to other systems.

(g) Use of the chat facility during a virtual lesson is permitted however you must ensure that the language used is appropriate. You should use the same language as you would use in the physical presence of a student. All chat is logged, both the public chat and private chats.

(h) When using our virtual lesson platform, students are restricted in what they can do by default. You must never unlock or remove these restrictions from students in such a way that would represent a safeguarding or data protection risk – for example, by allowing students to see other students, or allowing students to send personal messages to each other. If you are in doubt as to what students are able to do, contact your School ICT Technician.

(i) If a student makes a safeguarding declaration, or you suspect a safeguarding risk, during a virtual lesson, you must follow the Trust's Safeguarding Policy in the same manner as you would if physically present. You should be vigilant for safeguarding risks if a student is at home for a long period of time – you may be the student's only contact with school.

(j) You must not use the Trust's virtual lesson platform for non-Trust or school related business.

(k) If you are unable to use the virtual lesson platform, or it is not functioning properly, you must report this to your school ICT Technician or to the Network Managers.

(l) On occasion the Network Managers or school ICT Technicians may join a virtual lesson. This will be for the purposes of monitoring the functionality of the system. Their arrival and departure to your lesson may not be announced.

(m) If you suspect a security issue during your virtual lesson (for example, you believe a student is logged on as another student), you should inform the Network Managers at the earliest opportunity, so that an investigation can take place.

4.7 The following acts are prohibited in relation to the use of our ICT systems and will not be tolerated:

(n) Violating copyright laws

(o) Attempting to harm minors in any way

(p) Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity

(q) Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service

(r) Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)

(s) Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party

(t) Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.

(u) "Stalking" or otherwise harassing any user or employee

(v) Collection or storage of personal data about other users

5. Educating pupils about online safety

a) Pupils will be taught about online safety as part of the curriculum

b) In **Key Stage 1**, pupils will be taught to:

   a. Use technology safely and respectfully, keeping personal information private

   b. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

c) Pupils in **Key Stage 2** will be taught to:

   a. Use technology safely, respectfully and responsibly

   b. Recognise acceptable and unacceptable behaviour

   c. Identify a range of ways to report concerns about content and contact

d) By the **end of primary school**, pupils will know:

   a. That people sometimes behave differently online, including by pretending to be someone they are not

   b. That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

   c. The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

   d. How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

   e. How information and data is shared and used online

   f. What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

   g. How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

e) In **Key Stage 3**, pupils will be taught to:

   a. Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

   b. Recognise inappropriate content, contact and conduct, and know how to report concerns

f) Pupils in **Key Stage 4** will be taught:

   a. To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

   b. How to report a range of concerns

g) By the **end of secondary school**, pupils will know:

   a. Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

   b. About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

   c. Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

   d. What to do and where to get support to report material or manage issues online

   e. The impact of viewing harmful content

f. That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

g. That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail

h. How information and data is generated, collected, shared and used online

i. How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

j. How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

h) The safe use of social media and the internet will also be covered in other subjects where relevant.

i) Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Training

a) All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

b) All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

c) By way of this training, all staff will be made aware that:

d) Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

e) Children can abuse their peers online through:

a. Abusive, harassing, and misogynistic messages

b. Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

c. Sharing of abusive images and pornography, to those who don't want to receive such content

f) Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

g) Training will also help staff:

h) develop better awareness to assist in spotting the signs and symptoms of online abuse

i) develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up

j) develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

k) The Designated Safeguarding Lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

l) Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

m) Volunteers will receive appropriate training and updates, if applicable.

7. Review of policy

7.1 This policy is reviewed every three years by Invictus Education Trust Board of Trustees. We will monitor the application and outcomes of this policy to ensure it is working effectively.

Invictus Education Trust
Rules for Responsible Internet Use
For Students

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

- I will not share my password with anyone, or use anyone else's password. If I become aware of another individual's password, I will inform that person and a member of the school staff.
- I will use a 'strong' password i.e. one that contains letters (upper case and lower case), numbers and possibly symbols which I will change on a regular basis.
- I will use school equipment properly and not interfere with the work or data of another student.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- Before I use or connect my own equipment (mobile phone, iPod, non-school laptop/tablet etc.) I will check with a member of staff to see if that is allowed.
- I am responsible for all e-mail, chat, SMS blogs etc. that I post or send and will use language appropriate to the audience who may read them. I will be respectful in how I talk to and work with others online and never write or participate in online bullying. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help protect other students and myself.
- I know that posting anonymous messages and forwarding chain letters is forbidden.
- Any files attached to an email will be appropriate to the body of the email and not include any inappropriate materials or anything that threatens the integrity of the school ICT system.
- I will not download or bring into school unauthorised programmes, including games and music, or run them on school computers, netbooks or laptops.
- I will not access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- When using the internet including a 'chat room' facility, I will not give my home address or telephone/mobile number, respond to requests using SMS or even arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will always follow the 'terms and conditions' when using a site. I know content on the web is someone's property and I will ask a responsible adult if I want to use information, pictures, video, music or sound to ensure I do not break copyright law.
- I will think carefully about what I read on the Internet, question if it is from a reliable source before I use the information, crediting the source.
- When undertaking an activity related to a school based course, I will get permission from a teacher before I order online.

- I will not make audio or video recordings of another student or teacher without his/her permission.
- I will always check with a responsible adult before I share or publish created content of myself or others.

I am aware of the CEOP report button and know when to use it.
I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed: ____ Date: ______________________

Print Name: ____

Invictus Education Trust
Staff Acceptable ICT Use Policy
Rules for Responsible Internet use

This policy applies to all adult users of the Trust's systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Headteacher or the Network Managers. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Headteacher.

Any inappropriate use of the School's internet & e-mail systems, whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

The Trust has an obligation to monitor the use of the internet and e-mail services provided in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. The Trust reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our students, parents and staff is personal. You must treat all Trust information with the utmost care whether held on paper or electronically.

Official Trust systems must be used at all times. You may not use third-party systems or services for conducting school or Trust business without permission.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- Unauthorised access to computer material i.e. hacking;
- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- You may not download any software to the Trust's ICT Systems. If you wish for software to be installed, please request this from your school ICT Technician.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

You should not:

- Introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software
- Seek to gain access to restricted areas of the network
- Knowingly seek to access data which you are not authorised to view
- Introduce any form of computer viruses
- Carry out other hacking activities

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Internet and e-mail access is intended to be used for school business or professional development. Any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the Trust's business purposes which include the following:

- Providing evidence of business transactions
- Making sure the Trust's business procedures are adhered to
- Training and monitoring standards of service
- Preventing or detecting unauthorised use of the communications systems or criminal activities
- Maintain the effective operation of communication systems

In line with this policy the following statements apply:

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from, parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.

- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word ‘personal’ in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to some social networking sites is blocked on the school systems. However, a school can manage access by un-filtering specific sites, and Internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an ‘official’ school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.
- Social networking applications include but are not limited to:
  - Blogs
  - Any online discussion forums, including professional forums ○ Collaborative spaces such as Wikipedia
  - Media sharing services e.g. YouTube, Flicker ○ ‘Microblogging’ applications e.g. Twitter

When using school approved social networking sites the following statements apply:

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from students on social networking sites whilst they are of school age (until they have left year 13). The legal age for children to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their school email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection

or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.

- Postings should not be critical or abusive towards the school, staff, students or parents or used to place a student, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them ➢ It should not breach the schools Information Security Policy

Data Protection

The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the Trust to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the Trust. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the Trust’s premises or working remotely you must:

- Keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask your Headteacher.
- Familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions
- Familiarise yourself with all appropriate Trust Policies and Procedures
- Not make personal or other inappropriate remarks about staff, students, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable. I have read through and fully understand the terms of the policy. I also understand that the Trust may amend this policy from time to time and that I will be issued with an amended copy.

Signed: ____ Date: ____________________

Print Name: ____

Invictus Education Trust
Community User- Acceptable ICT Use Policy
Rules for Responsible Internet use

This policy applies to all community users of the Trust's systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.

The Trust has an obligation to monitor the use of the internet and e-mail services, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and the Trust reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- Unauthorised access to computer material i.e. hacking
- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.

You should not:

- Introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software
- Seek to gain access to restricted areas of the network
- Knowingly seek to access data which you are not authorised to view ➢ Introduce any form of computer viruses

I have read through and fully understand the terms of the policy. I also understand that the Trust may amend this policy from time to time and that I will be issued with an amended copy.

Signed: ____ Date: ________________________

Print Name: ____