

# E-Safety Policy

# **Embleton View**

#### Introduction

We have written our E-Safety Policy based on government guidance. All staff, across the service community contribute to the E-Safety Policy and the responsibilities are shared. Any technology used in service (regardless of ownership) shall be governed by this policy. Students also have responsibilities under this policy identified in the Acceptable Use Policies. This policy should also be read in conjunction with the Anti-Bullying Policy. Networked computer resources and internet access are widely available at Embleton View. They enhance the teaching and learning environment for both Learning and Development Coordinators (LDC), Learning Coaches (LC) and students, but are sophisticated and powerful tools and internet use in particular raises a range of legal, ethical, technical and management issues. There is therefore a need for proper regulation in the use of computers and internet by staff and students. This is provided in the service's ICT and internet policy contained in document. All those who wish to use the system must comply with this policy.

In accordance with legislative requirements there is annual update training for staff regarding esafety. The service also organises annually an awareness session for parents/guardians with regards to e-safety.

The schools Safeguarding and Child Protection policy outlines the school approach to keeping children safe from abuse online. Embleton View recognise that abuse can take place online, offline, or a combination of both. This policy outlines the practical measures implemented to keep children safe online.

### For students:

Students at Embleton View will be given supervised, monitored and filtered access to our computing facilities and will be provided with access to filtered internet (cisco umbrella) and other services operating at Embleton View. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of students. Key messages to keep student's safe are to be promoted and should be applied to both online and offline behaviours. The primary purpose of this Policy is to safeguard students and staff at Embleton View. It details the actions and behaviour required from students and members of staff in order to maintain an e-safe environment and is based on current best practice drawn from a wide range of sources.

# **Health and Safety Policy**

The safe use of ICT is included within the Health and Safety Policy, and also include guidelines for the use of display screen equipment. The detrimental impact of prolonged ICT use on children's brain development should also be addressed. Embleton View provides an environment in which students, parents/guardians and staff are safe from images being recorded and inappropriately used in turn eliminating the following concerns: staff being distracted from their work with students, the safeguarding of students from inappropriate use of mobile phone cameras and other digital



recording equipment. N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, iPod, iPad etc.

All staff, across the school community contribute to the E-Safety Policy and the responsibilities are shared. Any technology used in service (regardless of ownership) shall be governed by this policy. Students also have responsibilities under this policy identified in the Acceptable Use Policies. This policy should also be read in conjunction with the Anti-Bullying Policy. Networked computer resources and internet access are widely available. They enhance the teaching and learning for both LDC's and students, but are sophisticated and powerful tools and internet use in particular raises a range of legal, ethical, technical and management issues. There is thus a need for proper regulation in the use of computers and internet by staff and students. This is provided in the service's ICT Policy. All those who wish to use the system must comply with this policy.

# Why is Internet use important?

All students deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. In order for the school to maintain such an environment for students, everybody must be aware of the need to ensure online protection (E-Safety) and subsequently understand the principles of this policy and the expectations of service practice as documented below.

Having Internet access enables students to explore thousands of global libraries, databases and bulletin boards. They may also be to exchange messages with other students and education staff throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to students. In addition, students' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert the headteacher who will make the Director of Operations aware. He will tailor the filtering to suit the individual needs of subjects and the service generally. Although this filtering uses the latest security technology, parents/guardians need to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at Embleton View we believe that the benefits to students having access to the internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. Although, as with any other area, parents and guardians of minors along with Embleton View share the responsibility for setting and conveying the standards that students should follow when accessing and using these media information sources at service and/or at home. During school time, LDCs will guide students towards appropriate material on the internet. Outside service, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio etc.

### How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide



- Access to experts in many fields for students and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Improved access to technical support
- Exchange of curriculum and administration data with LA and DfE

#### How will students learn to evaluate Internet content?

- If staff or students discover unsuitable sites, The URL (address) and content must be reported to the LDC and then to the DO or Headteacher.
- Staff and students should ensure that their use of Internet derived materials complies with copyright law.
- Students should be taught to be critically aware of the materials they read and show how to validate information before accepting it's accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright.

# **Teaching and Learning:**

- The internet is an essential element in 21<sup>st</sup> 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The schools Internet access will include filtering appropriate to the age of students.
- Students will be taught what internet use is acceptable and what is not, and given clear objectives for Internet use.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and students complies with copyright law.

### **Access to Computers:**

- Access to the school network is available from any network station during the normal school day in lesson time with an adult supervising. Computer access is not available during school holidays.
- Intentional damage caused to a computer, computer systems or networks including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.
- The unauthorised access or use of personal information, contrary to the previsions of the GDPR is not permitted.
- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.



- Each computer has a 'student access' account which can be controlled by an IT administrator. The Student account will not be able to access any personal information gathered by Embleton View. Student work will be saved to these accounts.
- If a 'virus alert' occurs when transferring work from one mode to another the DO should be informed immediately. All external hardware e.g. Memory sticks must be vetted by submitting them to an anti-virus check.
- Students primarily have access to school chromebooks which are administrated centrally by the DO. This includes access settings and app download settings.
- Security strategies will be discussed at staff meetings.

# **Protecting Personal Data:**

 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

### E-mail Usage:

Students at Embleton View of service are given a service educational Gmail email account.

- Staff must not reply if they receive an offensive e-mail and must immediately inform a member of SMT.
- Students must not reveal details of themselves or others in e-mail communication or via a personal web space, such as their age, the location of the service, messaging account details, an address or telephone number, or arrange to meet anyone.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

# **Embleton View Website**

Photographs and videos may only be uploaded to the school website with the Directors approval. Student's names are never used on our website. Images of students may be used for promotional purposes but will never include any identifying text. Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

# Published content and the service website:

- Staff or student personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Student's full names will not be used anywhere on the school website or other on-line space.
- We will use photographs of student's work when communicating with parents/guardians and the wider community, in newsletters and in the service prospectus.
- Photographs will be checked to ensure that they are suitable (photos of students in swimwear would be unsuitable).
- Photographs used will not be captioned with student's names.



### **External Photographers**

Professional photographs may be taken throughout the year at school shows, by local media and Professional Service Portraits.

The Headteacher ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of children from inappropriate use of images.

# Social networking:

- The school will not allow access to social networking sites such as snapchat, instagram, Facebook or Twitter for students or staff unless done so for planned educational purposes.
- Disruptive sites that pose disturbance to learning or the learning of others will also be blocked. This may include Soundcloud, Tik Tok and even Youtube unless required for educational purposes.
- Students will be advised never to give out their personal details of any kind which may identify them, their friends or their location.
- Students and parents/guardians will be advised that the use of social network spaces outside school brings a range of dangers for primary aged students.
- Any students that make a disclosure of any malicious / inappropriate behaviour targeted towards them on social media will have the full support of school in dealing with the issue as any other safeguarding concern. This includes involvement of children or adults from outside the school.
- Staff will never post content to their personal social networking accounts that can identify Embleton View or any students. This includes doing so outside of work hours.
- All incidents of online child on child abuse will be reported to the DSL and managed appropriately.

# **Managing Emerging Technologies:**

- Emerging technologies will be examined by the Directors for educational benefit and a risk assessment will be carried out before use in service is allowed.
- ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, internet, online services and may also include personal ICT devices when used for service business. Where applicable, everybody should be aware of and review regularly, their responsibility when using ICT (as defined); service information systems; and electronic communicating with students. All users must adhere to the service's E-Safety policy and the Data Protection Act.

ICT in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in service and, more importantly in many cases, used outside of service by students may include:

- The Internet
- e-mail
- Instant messaging often using simple web cams



- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites (Popular: <a href="http://www.youtube.com/">http://www.youtube.com/</a>)
- Chat Rooms (Popular <u>www.teenchat.com</u>, <u>www.habbohotel.co.uk</u>)
- Gaming Sites (Popular <u>www.neopets.com,http://www.miniclip.com/games/en/,http://www.runescape.com/</u>/ http://www.clubpenguin.com)
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- VR Headsets
- Artificial Intelligence (ChatGPT etc)

### **Authorising Internet Access:**

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any service ICT resource.
- Embleton View will maintain a current record of all staff and students who are granted access to service ICT systems.
- Parents/guardians will be asked to sign and return a consent form.
- Any person not directly employed by the service will be asked to sign an 'acceptable use of service ICT resources' before being allowed to access the internet from the service site.

### **Assessing Risks:**

- We will take all reasonable precautions to prevent access to inappropriate 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 computer connected
   to the school network. The school cannot accept liability for any material accessed, or any
   consequences of Internet access.
- Emerging technologies, such as personal mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the e-Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.

# **PREVENT**

- All school computers have Mcafee Livesafe and Cisco Umbrella security installed. This is managed by a central admin account, which prohibits staff and students altering security settings.
- Each student has a school email address which enables them to access the school chromebooks or laptops. The school google G Suite has built in permissions per user based on age, which prevents access to unauthorised sites and content. This is managed centrally by the DO.



- Student accounts are protected using parental controls. These filter out any websites that include extremist content or links to extremist content.
- All students are supervised while accessing school computers. Any activity that could be considered extremist or showing signs of radicalisation is reported to the head teacher or DSL straight away.
- All staff are trained in PREVENT and can identify potential signs of radicalisation.
- All staff are aware of the CHANNEL process and their role in the early intervention of radicalised behaviour.
- Any students found to be accessing extremist content will be prevented from using the internet until a risk assessment has been completed.

### How will the policy be introduced to students?

- Rules for internet access will be posted in all rooms where computers are used
- Students will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede internet access
- Students will be informed that network and internet use will be monitored and appropriately followed up.

Consideration must be given as to the curriculum place for teaching e-Safety. It should be considered part of the pastoral programme and permeating other subjects. Useful e-Safety programmes can include:

- Think U Know; currently available for secondary students. (www.thinkuknow.co.uk)
- Grid Club www.gridclub.com
- The BBC's ChatGuide: www.bbc.co.uk/chatguide/

### How will staff be consulted and made aware of this policy?

- All new staff will be taken through the key parts of this policy as part of their induction
- All staff including LDCs and LCs will be provided with the services e-Safety Policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible internet use, and on the services internet policy will be provided as required
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read and sign Staff Code of Conduct prior to using service ICT equipment in the service

# How will monitoring and filtering & system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- McAfee Virus protection will be installed and updated regularly
- Cisco Umbrella implemented across all Wifi networks
- Wifi Routers managed by DO to ensure password protection against unauthorised devices.



- Personal data sent over the internet will be encrypted or otherwise secured
- Use of portable media such as memory sticks and CD-ROMs will be reviewed and its content can be searched by a member of staff.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the DO and kept in a secure place.
- Any unauthorised online interactions or material accessed by students will be referred to safeguarding in line with the schools child protection and safeguarding policy if deemed appropriate.

# How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a member of the Senior Managment Team
- Complaints of Internet misuse will be dealt with a the Headteacher
- Any complaint about staff misuse must be referred to the DO
- Complaints of a child protection nature must be dealt with in accordance with our child protection procedures.
- Students and parents/guardians will be informed of the complaint procedure
- Parents/guardians and students will need to work in partnership with staff to resolve issues
- As with drug issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

# How will Parents/guardians' support be enlisted?

- Parents/guardians' attention will be drawn to the responsible internet use policy in newsletters, and on the school website.
- Internet issues will be handled sensitively to inform Parents/guardians without undue alarm
- A partnership approach will be encouraged with parents/guardians and could include information booklets, practical sessions and suggestions for safe internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents/guardians.
- We will maintain a list of e-Safety resources for parents/guardians.

# **ICT Acceptable Use Policy**

# Acceptable use by Parents/guardians and carers

Partnership working with Parents/guardians and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable and unacceptable behaviour. Should Parents/guardians or carers wish to use personal technologies, such as cameras within the setting environment, authorisation must be obtained from the Senior Designated Person for Safeguarding or Headteacher. Specific guidelines for the use of such technologies must be followed.



### Acceptable use by visitors, contractors and others

All individuals are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with students. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.

### **Health and Safety:**

Since most ICT equipment is usually mains powered and may also be heavy, it represents a potential safety hazard and should be treated carefully. Portable equipment needs extra careful handling. In addition, most ICT equipment is considered to be Display Screen Equipment (DSE) and therefore falls under the relevant Health & Safety regulations.

# The following will apply:

- Do not use ICT without permission.
- Food and drink must not be consumed near any computer equipment anywhere in the school
- Do not move about the room while seated on a chair.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer faults should be promptly reported to DO. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.
- Mobile phones should not be used in service work time. Exceptions can be made for emergency contact at the Headteachers discretion

### At the end of a session:

- Log off/shut down according to instructions.
- Replace laptops as directed.
- Wind up and put away any headsets.

# **General Housekeeping:**

The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.

The following will apply:



- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.
- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

### **Security and Software Licensing:**

Security is especially important in schools, where vigilance is needed at all times to be ready to detect any forms of personal intimidation and exposure to inappropriate material. It is therefore very important that users' accounts are used only by themselves; otherwise they are exposed to impersonation by another user.

The following rules are industry standard:

- Always log out of your computer when you have finished, or if you have to leave it unattended.
- Do not let anyone else log in to a computer using your username and password.
- Do not tell anyone your password; you are responsible for keeping it secure.

The school uses up-to-date antivirus software on all computers; however, antivirus software is only as good as the latest virus definitions, which always lags behind the discovery of new virus threats. Therefore:

- Users must report any virus alerts they encounter to the DO.
- Users must report anything suspicious to a member of the SMT.

Installing software onto the service's computers is very carefully controlled and audited by the DO, in order that the school can be sure to be acting legally by not breaking licensing and copyright laws in respect of software. In addition, uncontrolled installation of software represents an unacceptably high security risk. Staff are not permitted to install software or programs onto computers without the prior authorisation of the Headteacher or DO.

# **Security on the Internet:**

The Internet can be a dangerous place. Not only can it provide access to material which might be considered inappropriate for certain audiences, but it can also be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this:

- Do not type any personal details (including your name or email address) into a web site
  unless you are absolutely sure of the authenticity and trustworthiness of the associated
  company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- Attempts to access the 'Dark Net' is prohibited.
- The use of internet-based email or newsgroups is prohibited except with the prior written approval of the Headteacher.



### **Accuracy of Information on the Internet:**

The internet contains a wealth of useful facts and information. However, most content on the internet is neither moderated nor regulated, therefore it is unwise to trust either the authenticity (that the material is written by the person it says it is) or the accuracy of information found on the internet. Do not automatically trust the accuracy or authenticity of information you find on the internet.

### **Downloading Material from the Internet:**

Much material on the internet is covered by copyright law and, unless specifically stated otherwise on the website, users may be breaking the law by downloading material. Do not download or copy any material from the Internet unless you are sure that the source is reliable and that there are no copyright, intellectual property right or licensing restrictions. If in doubt, ask the LDC or LC. In addition, it has already been stated in this policy that installation of software is prohibited.

### **Supervision:**

Access to the internet will be blocked to students outside of normal classes (i.e. during lunchtimes and after service). Students may be unblocked for a specific lunchtime or after-service session if a suitable justification for requiring access to the internet is accepted and there is a member of staff available to supervise. During normal lesson time it is expected that staff will supervise access to the internet.

### **Recreational Use of the Internet**

Access to the internet is provided to support the curriculum, support service administration and for staff professional development only. Recreational or personal use of the internet is not permitted except with the prior written approval of the Headteacher. It will be considered a disciplinary issue if staff access the internet for personal use during service time. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in service is allowed.

#### **Sanctions:**

Students/staff found not to be abiding by this policy may be subject to sanctions. Violations of the school ICT and internet Policy will result in a temporary or permanent ban on your use of the school network or of the internet. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour

When applicable, the school may be under obligation to involve police or the LA.

### **Legal Issues:**

The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer".



The school wishes to make it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised".

# **Service-Parent-Student and Staff Agreements:**

The school will use agreements, signed by parent/carer in order to convey the importance of the issues and to signify that the essential elements of the Acceptable Use Policy have been read. The agreement will also serve as a consent form for parents/guardians/carers to give permission for students to use the ICT facilities and, more particularly, access the internet. The agreement will be distributed to all students when they first start at the school, together with the ICT e-safety rules. Significant updates to the policy and/or the agreement may necessitate its redistribution and resigning.

# Applies to:

- The whole school and all other activities provided by the school, inclusive of those outside of the normal school hours;
- All staff (teaching, support and admin staff), students on placement, the proprietors, Board of Directors, agency staff and volunteers working in the school.
- Visitors and contractors accessing the site.

# **Availability**

 This policy is made available to parents, staff and students as a hardcopy upon request from the school office.

### **Monitoring and Review:**

- This policy will be subject to continuous monitoring, refinement and audit by the Headteacher.
- The Headteacher and/or the Board of Directors and/or a suitably appointed delegate will
  undertake a formal review of the policy, by no later than two years from the date shown
  below, or earlier if significant changes to the systems and arrangements take place, or if
  legislation, regulatory requirements or best practice guidelines so require.

# Legal Status;

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England)
   Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- Keeping Pupils Safe in Education (KCSIE) Information for all schools and colleges (DfE: September 2022) incorporates the additional statutory guidance, Disqualification under the Childcare Act 2006 (February 2015) and also refers to non-statutory advice for teachers, What to do if you're worried a child is being abused (HM Government: March 2015)
- Working Together to Safeguard Pupils (WT) (HM Government: 2015) which also refers to non-statutory advice, Information sharing HM Government: March 2015); Prevent Duty Guidance: for England and Wales (March 2015) (Prevent). Prevent is supplemented by The



Prevent duty: Departmental advice for schools and childminders (June 2015) and The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE )

- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'
- Prepared with reference to DfE Guidance (2014) Preventing and Tackling Bullying: Advice for school leaders and governors and the relevant aspects of Safe to Learn, embedding antibullying work in schools.
- Having regard for the guidance set out in the DfE (Don't Suffer in Silence booklet)
- The Data Protection Act 1998; BECTA and CEOP.

#### **Related Documents:**

- Child Protection and Safeguarding
- PREVENT Policy
- Data Protection Policy
- Data Retention Policy
- Acceptable Use of Mobile Devices Policy

a. bum	MU
Graeme Turner	Craig Bell
(Proprietor)	(Proprietor)
Date: 02/08/17	Date: 02/08/17, 27.07.20, 05/01/21,
	28.07.21, 29.6.22, 06/07/23