Part 1

Name of policy	**E-Safety**
Status of policy	This is a non-statutory policy
Consultation	This policy has been developed in consultation with Governors, Senior Leadership Team and Staff and Pupil Council.
Relationship with other policies	This policy should be read in conjunction with C1 Curriculum policy; P4 Safeguarding and Children Protection Policy; P6 Student Behaviour Policy; P7Anti-Bullying Policy; F5 Freedom of Information and Data Protection
Date policy was agreed	12th June 2017
Date for full implementation	Immediate
Date for review	Annually

Part 2

Policy

1. Edgbarrow School recognises that new technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.

2. This policy applies to all members of the school community (including staff, students, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. (See Appendix 1 and 2)

3. The Governing Body aims to ensure that children and young people are able to use The Internet and related communications technologies appropriately and safely and this is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

4. Learning
   a) Why the Internet and digital communications are important
      - The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.
      - Internet use is an essential part of the curriculum and a necessary learning tool for staff and pupils.

   b) Internet use will enhance and extend learning
      - Staff will be made aware of and pupils will be educated in the safe use of the Internet
      - Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.

   c) Pupils will be taught how to evaluate Internet content
      - The school will ensure that the use of Internet-derived materials by staff and by pupils complies with copyright law.
      - Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
      - Pupils will be made aware of how they can report abuse and who they should report abuse to.
      - Pupils will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
      - Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

   d) Managing monitoring and filtering
      The school will work in partnership with Bracknell Forest Council to ensure that systems to protect pupils are reviewed and improved.
      - If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Leads or

the Systems Manager.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- All Internet activity is logged by the school's Internet provider. These logs may be monitored by authorised Edgbarrow School staff.

e) Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- No pupils or staff should interfere with any anti-virus software installed on school ICT equipment.
- Machines not routinely connected to the school network must be updated regularly with virus updates by ICT Support.
- If a virus is suspected on any school ICT equipment, use of the equipment should be stopped immediately and the Systems Manager contacted immediately. The Systems Manager will advise the actions to be taken and be responsible for advising others that need to know.

f) Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. The school will monitor this and continue to research solutions to this potential issue.
- For KS3 mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate messages is forbidden.

g) Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software, and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that needs to be reviewed prior to implementing such a policy.
Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing, and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe

- Mandatory training is undertaken for all Staff / Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

h) Protecting personal data
- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.
- Staff will so far as possible not leave any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked with a pin code and kept out of sight
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan, and copiers) are used.

5. Managing Internet Access

a) Information system security
- School ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

b) E-mail
- Pupils and staff should only use approved school e-mail accounts at forename.surname@edgbarrowschool.co.uk
- Pupils and Staff must be made aware of how they can report abuse and who they should report abuse to.
- Pupils and Staff must report if they receive an offensive or inappropriate e-mail.
- In e-mail communications, pupils and staff must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from the relevant line manager.

c) Published content and the school VLE
- Staff or pupil private and personal contact information will not be published. The contact details of staff provided will be the person's official school e-mail address.

d) Publishing students' images and work
- Written permission, using the approved permission forms, from parents or carers, will be obtained before photographs of pupils are published on the school Website/ VLE, social media, and any other publications.

e) Social Media and personal publishing
- The school will educate people in the safe use of social media, including Facebook and Twitter.

- Staff using social media for school purposes must use the agreed platforms used by the school
- Staff wanting to set up departmental sites or pages can do so in consultation with the E-Learning Manager who will be able to monitor content posted
- The staff is not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher

f) Arrangements for Monitoring & Evaluation

The success of this policy and e-safety provision is maintained by the Systems Manager and the E-Safety Leads in the school - Designated Senior Person and the SLT Line Manager for ICT. It will be monitored and evaluated through:

- SIMS behavioural reports
- IT filtering systems
- The tracking of security breaches/data loss

g) CCTV

- The school uses CCTV for security and safety. The only person with access to this is the schools Facilities Manager**.** Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school

6. Policy Decisions

a) Authorising Internet access

- All staff, governors, and visitors must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource, including any laptop issued for professional use.
- The school will maintain a current record of all staff, governors, visitors and pupils who are granted access to school ICT systems.
- Secondary age pupils must apply for Internet access individually by agreeing to comply with the school's ICT Acceptable Usage policy by signing relevant pages in the student diary.

b) Assessing risks

- The school 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. Neither the school nor Bracknell Forest Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

c) Prevent Duty

- Edgbarrow School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.
- We take reasonable measures to protect pupils from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material.
- Our Safeguarding and e-Safety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

d) Handling e-safety complaints

- Complaints of Internet misuse will be reported to the Senior Information Risk Owner and action in-line with the Bracknell Forest Safeguarding Children Board e-Safety policy will be taken.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that a member of staff is unsuitable to work with children should be reported to the Designated Senior Person within one working day in accordance with Bracknell Forest Council Safeguarding Board policies.
- Any complaint about staff misuse must be referred to the head teacher and if the misuse is by the head teacher it must be referred to the chair of governors in line with Bracknell Forest Council Safeguarding Board Child Protection procedures.
- Pupils, parents and staff will be informed of the complaints procedure.

7. Communicating e-Safety

a) Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used.
- All system users will be informed that network and Internet use will be monitored.
- A programme of e-Safety training and awareness raising will be put in place in-line with the Bracknell Forest Council Safeguarding Children Board's e-Safety Strategy.

b) E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety**.**

- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the relevant legislation when using the Internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images

and other important areas through discussion, modeling, and appropriate activities.

c) Staff and the e-Safety policy
- All staff will be given access to the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- The staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

d) Enlisting parents' and carers' support
- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will hold parent/carer information sessions on e-safety.

Staff, Governor, and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, The Internet, and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff is aware of their professional responsibilities when using any form of ICT. All staff is expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with our School e-Safety coordinator (Lucy Stockwell) or Senior Information Risk Owner (Gareth Croxon).

- I will only use the school's email / Internet / Intranet / Learning Platform/Social Media and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities and will ensure that I log out of or lock the school system when not in use.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of Systems Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the staff member. Images will not be distributed outside the school network without the permission of the member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and ICT Acceptable Usage policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- Staff who have been issued with ICT equipment will return item/s when no longer employed by the school.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……..…… Date ……

Full Name ……..... (printed)

Job title ……

Appendix One B

Regulations for the Use of ICT Facilities - Staff

These regulations apply to the use of all Internet and electronic mail facilities, access to the MIS through the SLG multi-user computers, workstations and laptops, and any networks connecting them provided by the school. Staff in breach of these regulations may find themselves subject to disciplinary action.

The facilities must always be used responsibly in connection with learning or other purposes permitted by the Head that does not interfere with the working day. Staff must not interfere with the work of others or the system itself; under no circumstances may the facilities be used for commercial gain.

Staff user accounts are for their sole use and under no circumstances must pupils be given access to these. Staff must not gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people.

The examples below are not an exhaustive list of concerns but are only given to explain a number of issues that the school faces.

In particular, staff must not:	Examples
• Create, transmit or cause to be created or transmitted material which is designed or likely to cause damage, annoyance, inconvenience, needless anxiety or offence and you must not create, transmit or cause to be transmitted offensive, obscene or indecent material.	• Sending unpleasant or threatening email messages to other members of the school community and beyond. • Using and responding to offensive language on screen. • Creating offensive animations. • Accessing inappropriate websites, including pornography, crime, firearms. • Knowingly introducing a virus or other software which may cause damage or destruction to data or hardware.
• Create, transmit or cause to be created or transmitted defamatory material or material which infringes the copyright of another person.	• Sending emails or creating web material that spreads rumours, gossip and lies.
• Gain deliberate unauthorised access to facilities or services accessible via local or national networks.	• Entering and using anyone else's user area unless authorised to do so by the systems manager. • Registering your own or other staff email addresses for goods and services you are not eligible for e.g. gambling etc. • Downloading software and 'add-ins' directly or from host sites as these can carry viruses which could infect our network.
• Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means.	• Communicating with pupils via (although not exclusively) any of the following media: SMS text message, email that is not through the school email system, instant messaging or telephone. • Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.
• Inadvertently or deliberately allow any member of the public or family member to have access to confidential pupil information or school data through online sources or portable media.	• Allowing non-staff members' access to the SIMS Learning Gateway. • Inadvertently allowing non-staff members to view or access material by failing to log out of a data website or by leaving usernames and passwords on view. • Inadvertently showing confidential and personal information on whiteboards.

ICT Acceptable Use Agreement

In the context of the schools ethos of trust, it is important for us to clarify our expectations with regard to the use of ICT equipment in conjunction with the laws relating to data protection, e-safety, and computer misuse. Although we do not think your child is likely to break any of the rules set out below, we feel it is important that you stress upon him/her the importance of not abusing the trust placed in them. Please discuss the following points with your child and sign to acknowledge your acceptance of this agreement.

1. I will only use ICT systems in school, including The Internet, e-mail, digital video, and mobile technologies and social media, for school purposes.
2. I will not damage ICT equipment in any way. If I cause non-accidental damage I will be responsible for the costs of the repair.
3. If I discover a piece of faulty ICT equipment I will report it to a member of staff before I log on to it.
4. I will not download or install software on school technologies.
5. I will only log on to the school network, other systems, and resources with my own username and password.
6. I will follow the school's ICT security system, will not reveal my passwords to anyone and will change passwords when prompted.
7. I will make sure that all ICT communications with students, teachers or others are responsible and sensible.
8. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
9. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher or Head of Year.
10. I will not give out any personal information such as name, phone number or address to anyone I do not know.
11. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
12. Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network without the permission of the E-Learning and Communications Manager.
13. I will ensure that my online and social media activity, both in school and outside the school, will not cause distress to any member of the school community and will not bring the school into disrepute.
14. I will support the school's approach to online safety, the use of social media and will not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
15. I will respect the privacy and ownership of others' work online at all times.
16. I will not plagiarise (copy) the work of others and present it as my own.
17. I will not attempt to bypass The Internet filtering system.
18. I understand that all my use of The Internet and other related technologies can be monitored, logged and made available to my teachers.
19. I must not allow another student to use their personal device
20. I must respect a teacher's wishes on when they can use their devices
21. If a device is lost on the school site I must report it to my Tutor or Head of Year immediately
22. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my Parent/Carer may be contacted. In extreme cases, my access to the school ICT facilities could be withdrawn and further legal action may be taken.

Name of student ……..…..... Form …….

Signature of student ……..……..……..

Signature of Parent/Carer ……..…….…….

- **Appendix Two B**

Regulations for the Use of ICT Facilities - Pupils

These regulations apply to the use of all Internet and electronic mail facilities, multi-user computers, workstations and laptops, and any networks connecting them provided by the school.

The facilities must be used only in connection with learning at school or other educational purposes permitted by the Head and domestic communication with friends and family. Use of Internet chat services such as MSN and 'Yahoo Chat' is forbidden owing to the inability to filter out undesirable callers.

Pupils **must not** interfere with the work of others or the system itself. The facilities must be used in a responsible manner. Under no circumstances may the facilities be used for commercial gain. Pupils' user accounts are for their sole use. Pupils **must not** gain unauthorised access to or violate the privacy of other people's files, corrupt or destroy other people's data or disrupt the work of other people.

In particular pupils must not:	Examples
• Create, transmit or cause to be created or transmitted material which is designed or likely to cause damage, annoyance, inconvenience, needless anxiety or offence and you must not create, transmit or cause to be transmitted offensive, obscene or indecent material.	• Sending unpleasant or threatening email messages to other members of the school community and beyond. • Using and responding to offensive language on screen. • Creating offensive animations. • Accessing inappropriate websites, including pornography, crime, firearms. • Knowingly introduce a virus or other software which may cause damage or destruction to data or hardware.
• Create, transmit or cause to be created or transmitted defamatory material or material which infringes the copyright of another person.	• Sending emails, photographs or videos or creating web material that spreads rumours, gossip, and/or lies. • Copying information directly from other sources and presenting it as your own.
• Use networked computing equipment for playing computer games.	• Playing unauthorised computer games.
• Gain deliberate unauthorised access to facilities or services accessible via local or national networks including proxy bypass sites.	• Entering and using anyone else's user area, including changing passwords and deleting or tampering with another user's work. • Registering your own or other pupils' email addresses for goods and services you are not eligible for e.g. lotteries, loans etc. • Making purchases on The Internet. • Downloading software, music/video and 'add-ins' directly or from host sites or by opening email attachments, especially games or 'cheats' as these can carry viruses which could infect our network. • Accessing blocked sites via a proxy bypass website.

Pupils in breach of these regulations may find their access withdrawn and persistent or extreme misuse of the network could lead to an exclusion from school.

Appendix 4


E
E-Learning
I will only use ICT systems in school for school purposes
I will respect the privacy and ownership of others' work online at all times
I will not damage ICT equipment in anyway
D
Discipline
I will log on to the school network, systems & resources with my own user name & password
I will not attempt to bypass the Internet filtering system
I understand that all my use of the Internet and other related technologies can be monitored
I will not touch anyone else's keyboard or mouse without their permission
G
Get Wise
I will follow the school's ICT security system and will not reveal my passwords to anyone
I will be responsible for my behaviour when using the Internet
If I discover a piece of faulty ICT equipment I will report it to a member of staff
S
Safe
I will not give out any personal information such as name, phone number or address to anyone I do not know
I will not arrange to meet someone unless this is part of a school project approved by my teacher
A
Advice
I will ensure that my online and social media activity, both in school and outside school, will not cause distress and will not bring the school into disrepute
Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy
F
Fraud
I will not deliberately browse, download, upload or forward material considered offensive or illegal
I will not download or install software on school technologies
I will not plagiarise (copy) the work of others and present it as my own
E
e-Safety
I understand these rules are to keep me safe & school sanctions will be applied if not followed
I will make sure that all ICT communications with the community is responsible and sensible
I will support the school's approach to online safety and the use of social media