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 Student Council.

Relationship with other policies	This policy should be read in conjunction with
	C1 Curriculum policy;
	CLT P1 - Safeguarding and Child Protection Policy;
	P6 Student Behaviour Policy;
	P7Anti-Bullying Policy;
	F5 Freedom of Information
	CLT Data Protection Policy
	CLT Privacy Notice

Date policy was agreed	15th May 2023
Date for full implementation	Immediate
Date for review	Annually – May 2024

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 students 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 of all digital communications media.

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 students 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 students.

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

   c) Students will be taught the underpinning knowledge and behaviours that can help students to navigate the online world, regardless of device, platform or app. This includes:
      - How to evaluate what they see online.
      - How to recognise techniques used for persuasion.
      - Acceptable and unacceptable online behaviour.
      - How to identify online risks. In particular,
        - Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
        - Students 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.
        - Students 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
        - Students will be taught about online safety and harms, including what positive, healthy and respectful online relationships look like.
      - How and when to seek support including how they can report abuse and to whom they should report abuse.

- How online media link to wider concepts of democracy, freedom, rights and responsibilities.

d) The school will ensure that the use of Internet-derived materials by staff and by students complies with copyright law.

e) Managing monitoring and filtering:
The school will work with Corvus Learning Trust to ensure that systems to protect students are reviewed and improved.

- If staff or students discover an unsuitable site, it must be reported to the e-Safety Leads or the IT Systems Line 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.

f) 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 students or staff should interfere with any anti-virus software installed on school ICT equipment.
- School devices not routinely connected to the school network must be updated regularly with anti-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 Network Manager contacted immediately. The Network Manager will advise the actions to be taken and be responsible for advising others that need to know, including the IT Systems Line Manager if required.
- All actions will be logged for future review.

g) 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.
  - All use of student personal devices in lessons will be at teacher discretion. See behaviour policy.
- The sending of abusive or inappropriate messages is forbidden.

h) 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 greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that needs to be considered; the BYOD annex contains further guidance. In particular:

- BYOD users must still follow the school Acceptable Use Agreement,
- BYOD users must still follow the shool Data Protection guidance.
- Users must agree to the monitoring and filtering of their Internet usage while using the school network.

i) Protecting personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 2018 and related legislation.
- Detailed guidance is included in CLT Data Protection Policy and CLT Privacy Notice.

j) Remote Learning

Remote learning is a rapidly changing environment, as new technologies and tools are developed in response to the needs of schools. Detailed guidance will be provided in the Remote Learning Annex. In general, remote learning should adhere to the following principles:

- Any new remote learning tools must be approved by the e-safety team and the DPO before they are used with students.
- Students will be given instructions on how to use any remote learning technologies safely.

5. Managing Internet Access

a) Information system security

- School ICT system security will be reviewed regularly.
- Virus and malware protection will be installed and updated regularly.

b) Use of IT systems

- 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.
- Regular audits and monitoring of usage will take place to ensure security.

c) E-mail

- Students and staff should only use the school e-mail accounts provided. These normally follow the format: forename.surname@edgbarrowschool.co.uk.
- Students and Staff are made aware of how they can report abuse and to whom they should report abuse.
- Students and Staff must report if they receive an offensive or inappropriate e-mail.
- In e-mail communications, students and staff must not reveal their personal details or those of others.

d) Published Content

- Staff or student 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.

e) Publishing students' images and work

- Written permission, using the approved permission forms from parents, carers or students as appropriate to the age of the student, will be obtained before photographs of students are published on the school website, social media, and any other publications.
- Students will be asked for consent before their work is published or displayed.
  - Where work is displayed, the student's name should be given as their first name and the initial of their surname, rather than their full name.

f) Social Media and personal publishing

- The school will educate people in the safe use of social media.
- 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 & Communications Manager who will be able to monitor the content posted.
- The staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, 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.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher.

g) Arrangements for Monitoring & Evaluation

The success of this policy and e-safety provision is maintained by the Network 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.

h) CCTV

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- See CCTV policy.

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
- Access to our network and Internet services is monitored and recorded.
- Secondary age students must apply for Internet access individually by signing the school's ICT Acceptable Usage policy.

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 the Corvus Learning Trust 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 students. Every member of staff recognises that safeguarding against radicalisation and extremism is no different from safeguarding against any other vulnerability in today's society.
- We take reasonable measures to protect students 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
- Students, parents and staff will be informed of the complaints procedure.

7. Communicating e-Safety

a) Introducing the e-Safety Policy to Students

- 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 students 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 students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Students 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.
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling, 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 students 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
Edgbarrow School IT: Acceptable Use Policy

Edgbarrow School IT: Acceptable Use Policy

The school provides various IT systems in school to support staff and students with their work. This includes the use of PCs and laptops, access to the internet and a school email address; the school email may provide access to other online services, such as Google Classroom.

Staff accessing any school IT systems, including cloud systems such as email, must comply with all the school's IT security and online safety rules and guidance.

Staff accessing personal data, especially sensitive or protected data, must follow the data protection guidance and training provided.

For any questions about our IT systems, including online safety and data protection, please contact: phil.marshall@edgbarrowschool.co.uk

Staff should behave in an appropriate manner online. Online interactions should be **respectful, safe and positive.**

The Acceptable Use policy is designed to keep students and staff safe, including protecting our systems and data. Breaches of the policy will be addressed by the Headteacher, following the School disciplinary policy. In extreme cases, access to the school IT facilities could be withdrawn and further legal action may be taken.

The key points and rules are listed on the next page. Staff should discuss the rules together and sign to acknowledge their acceptance of this agreement. Staff not agreeing to, or following, the policy may have their access to school IT systems removed.

IT systems change regularly, so we may update our guidance during the school year. In this case, updated guidance will be posted to the IT CPD site and the updates will be publicised. Staff must complete annual or biannual training in e-safety, data protection and safeguarding as required by the school.

Please read the rules on the next page and the security guidance carefully. By ticking the digital signature box on the policy portal, you acknowledge that you have read and understood the School IT policy, and you agree to follow the rules and guidance provided.

Edgbarrow School IT: Acceptable Use Policy

1. I understand that I am responsible for looking after any personal data or confidential information that I access for school purposes. This includes digital data and printed materials.
2. I will follow the security rules and guidelines provided by the school to keep our data and systems secure. This includes disposing of personal data securely when it is no longer needed.
3. I will ensure that any personal devices I use for remote working or school purposes have adequate security. Security guidance will be sent at the start of each year.
4. I will not download or install anything, include software and add-ons, to school devices or services. Requests for software and add-ons (extensions) should be directed to IT Support https://support.tricomputers.co.uk/index.php
5. I will not share school data, including personal information about students, parents or staff, with any external service or company without first contacting the Data Protection Officer here: dpo@dataprotection.education or here: phil.marshall@edgbarrowschool.co.uk . I understand that all new IT systems and services must have been through a privacy impact assessment before use.
6. I understand that all my use of the internet and IT in school can be monitored, logged and made available to SLT. Staff should avoid using school IT systems for non-school purposes.
7. I will not reveal my password(s) to anyone and I will change my passwords when prompted. Passwords must meet the minimum-security standards set by the school.
8. 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 IT Support.
9. I will not attempt to bypass the internet filtering system or other IT security by any means.
10. I will not create or share any media, including images or video, that could upset any member of the school community. This includes taking photos or videos or staff or students without their consent.
11. I will not share anyone's personal information, such as their name, phone number or address without their consent.
12. I will report any security issues, inappropriate material or unacceptable behaviour to the Data Protection Officer or IT support. This includes reporting misuse of IT by students.
13. If I have any questions or concerns about IT security or online safety, I will contact phil.marshall@edgbarrowschool.co.uk or the Data Protection Officer: dpo@dataprotection.education

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 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 students 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 IT Systems Line 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 student who is not a member of their direct family, by any means.	• Communicating with students 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 student 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.

Student ICT Acceptable Use Agreement

IT Acceptable Use Agreement

The school provides various IT systems in school to support students with their work. This includes the use of PCs and laptops, access to the internet and a school email address; the school email may provide access to other online services, such as Google Classroom.

Students using any school IT systems must comply with all the school's IT security and online safety rules and guidance, which can be found here: https://www.edgbarrowschool.co.uk/students/online-resources/

For any questions about our IT systems, including online safety, please contact: help@edgbarrowschool.co.uk

Students should behave in an appropriate manner online. Online interactions should be **respectful, safe and positive**.

The IT rules are designed to keep students safe. If they are not followed, school sanctions will be applied and Parent/Carers will be contacted. In extreme cases, access to the school IT facilities could be withdrawn and further legal action may be taken.

The key points and rules are listed on the next page. Parents/Carers and students should discuss the rules together and sign to acknowledge their acceptance of this agreement. Students not agreeing to, or following, the acceptable use policy may have their access to school IT systems removed.

IT systems change regularly, so we may update our guidance during the school year. In this case, updated guidance will be posted to the school website and the updates will be publicised.

We have read the IT rules on the next page and the latest guidance on the Edgbarrow website. We understand and agree that these rules and guidelines are important to keep students safe when using school IT resources. We understand and agree that students who do not follow these rules may receive a sanction and/or lose access to our IT systems. We acknowledge that updates may be posted to the school website and we will read these when prompted.

Name of student…………………………………….. ………Form ………………

Signature of student ………………………… Signature of Parent/Carer ………………………

Date ……………………………………………

IT Acceptable Use Agreement: Rules for Students

1. I will only use IT systems provided by the school, including internet access, e-mail, digital storage, mobile technologies, cloud services, and social media, for school purposes.
2. I will not damage school IT equipment or services in anyway. If I cause non-accidental damage I will be responsible for the costs of the repair.
3. I will not download or install anything, include software and add-ons, on school devices or services.
4. I will only log on to the school network, other systems and resources with my own user name and password.
5. I will not reveal my passwords to anyone and I will change my passwords when prompted.
6. I will make sure that all IT communications with students, teachers or others are responsible and sensible. This includes the use of comments and chat in Google Classroom.
7. I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use. I will not engage in online harassment or cyber bullying.
8. 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.
9. I will not attempt to bypass the internet filtering system or other IT security by any means.
10. I understand that all my use of the internet and IT in school can be monitored, logged and made available to my teachers.
11. I will not create or share any media, including images or video, that could upset any member of the school community. This includes taking photos or videos or staff or students without their consent.
12. I will not share anyone's personal information, such as their name, phone number or address without their consent. I will be cautious about sharing my own personal data online and will seek advice if I am unsure about what I should share.
13. I will report any security issues, inappropriate material or unacceptable behaviour to help@edgbarrowschool.co.uk, my Head of Year or my IT/computer science teacher.
14. If I have any questions or concerns about IT security or online safety, I will contact help@edgbarrowschool.co.uk or my Head of Year or my IT/computer science teacher.

- ## Appendix Two B

Regulations for the Use of ICT Facilities - Students

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.

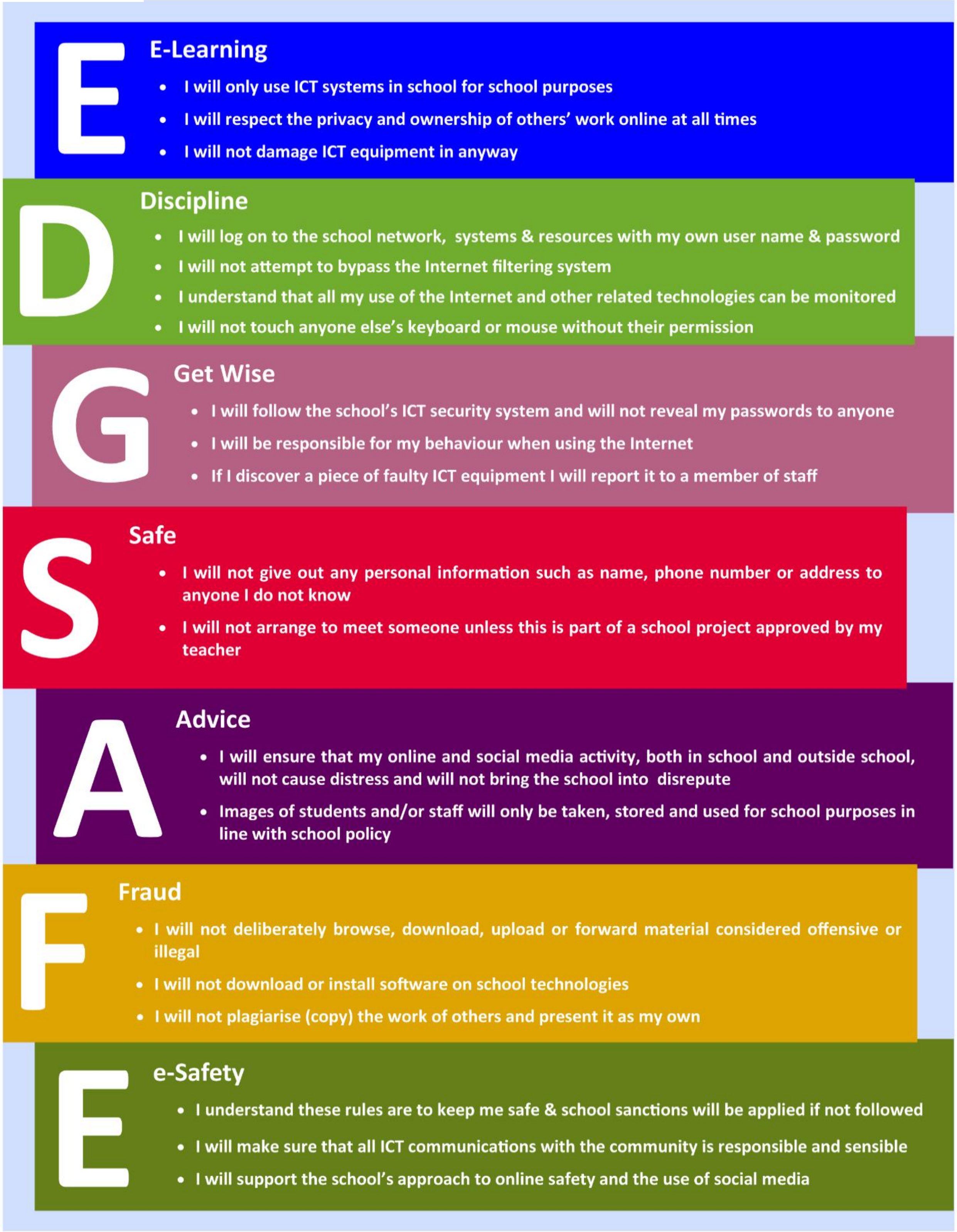
The facilities must be used only in connection with learning at school or other educational purposes permitted by the Head and domestic communication with friends and family. Use of Internet chat services such as MSN and 'Yahoo Chat' is forbidden owing to the inability to filter out undesirable callers.

Students **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. Students' user accounts are for their sole use. Students **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 students 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 students' 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.

Students 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-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

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

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

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

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

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-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

Appendix 5: Remote Teaching Guidance

This appendix summarises the advice given to staff, students and parents regarding remote teaching at Edgbarrow School. The circumstances surrounding remote teaching change regularly, as do the tools available to deliver remote learning, and so this appendix must be a living document. Further advice and guidance on using specific tools and products will be issued separately as appropriate.

For the purposes of this guidance, remote teaching includes:

1. On-demand content, such as videos and self-marking tasks, that students can access online in their own time
2. Delivering "live" lessons using online meeting software which allows a teacher to work with a group of students in real time without being in the same room

Point (1) is already part of our curriculum offer and is covered by our existing policies; the advice is summarised here for completeness and clarity.

Point (2) is new to the School and merits additional guidance and clarification to supplement the existing policies.

General Principles

Our main way of working remotely is Google Suite for Education, centred around Google Classroom. All students use this platform in KS3 IT and Computer Science and so it is a natural starting point for our online teaching and learning. We expect the majority of online learning, whether that is live lessons or accessing on-demand content to take place through Google Classroom.

Even if other online sources and tools are used, good practice is to set the work through Google Classroom so that students have a single point of reference for their online work.

In some cases, mainly A-level classes, some teachers may want to use Microsoft Teams. This is acceptable and the points in this document apply to MS Teams as well as Google Classroom.

Note that we have data protection policies in place already for the use of Microsoft and Google products, including YouTube (which is owned by Google), and other resources that are already used in lessons. However, we may not have data protection in place for other services.
Therefore, teachers must not use new online services without first contacting the Data Protection Officer (DPO), as per any new online service.

A key principle of our approach is to maximise access for students and avoid increased educational gaps between groups of students. We want to ensure high-quality online provision, while not disadvantaging students who do not have regular or reliable access to the Internet.

Students and parents/carers may use the email address help@edgbarrowschool.co.uk to request technical advice or support with our online services.

1. On-Demand Content

On-demand content includes, but is not limited to:

- Videos of lessons or instruction by staff
- Content or tasks narrated by staff, such as a commentary to accompany a presentation
- Video or audio feedback on work
- Interactive lessons or tasks, whether created by staff or by a third party

There is no expectation for staff to provide any particular form of online learning. We acknowledge that every member of staff has different circumstances and may not have access to the tools to create specific online content, such as videos of lessons. The School does not provide IT equipment for staff and there is no expectation that staff will buy equipment for work purposes.

Online provision should follow our existing teaching and learning policies including:

- Expectations regarding workload for both students and staff
- Expectations regarding marking and feedback
- Access arrangements for students

Online learning carries a risk of increased workload and pressure for both staff and students. Therefore, staff and students will receive guidance on managing their online work, including maintaining separation between work and home life.

1.1 Applications provided by the school

All students are provided with a school email address and access to the following services;

- Google Suite for Education, including
  - Google Classroom for accessing work
  - Google Drive for storing work
  - Google Docs (and related products) for working with documents
  - Google Meet for online meetings (discussed in part 2)
- Office 365, including
  - Outlook for email
  - Word online (and related products) for working with Office documents
- YouTube, which is owned by Google

These are cloud-based, so there is no requirement for students to have local access to any software at home.

We recommend that, for assignments which are going to be accessed by a member of staff, students use Google Docs, Google Drive and Google Classroom to create, edit, store and share work. This will allow staff and students to access work with fewest issues.

1.2 Third-party applications, i.e. software not provided by the School

Many subjects also use online textbooks and other third-party applications. Where these require a login, these are created using the students' school email addresses. These applications are already covered by our existing data protection policy and privacy notice.

If a member of staff wishes students to access a **new application**, then they must notify the DPO, who will check the relevant data protection and privacy notices. It may be easier for the E-Learning or IT team to manage some applications and logins centrally, so the E-Learning and IT teams should also be informed.

Apart from a small number of exceptions, chiefly relating to the sixth form and UCAS/careers, students should access services for lessons using their school email address. If an application requires additional details, students may provide the school details rather than personal data, if appropriate.

Staff will explain the use of any new applications to students and including any guidelines for signing up to or using the application.

When considering the use of a new application, staff should ensure that it is accessible to all students. For example, software that only runs on MS Windows or software that requires a particular web browser may not be accessible to all students. Staff should consider whether its use is necessary and whether a suitable alternative exists.

1.3 Publication of Content

Staff may wish to create videos of lessons or other instruction and this is often useful to students.

Staff may use whatever tools they wish to create this content, such as recording a Google Meet or narrating a PowerPoint presentation.

Ideally video content will be shared via Google Classroom so that students can access it using their existing logins and the applications with which they are familiar. We do not recommend emailing video files, due to their large size; video will not play correctly over our remote desktop service.

In some cases, it may be more convenient to publish videos to YouTube and share the link via Google Classroom. In this case, staff should observe the following:

- Staff should only publish school content that is to be accessed by students using their school YouTube account
- Content should be made private and shared with Edgbarrow School members
  - This will require students to sign in with their Edgbarrow login before viewing the video
- Staff should observe copyright and other guidance as per any other school resource
- Staff should refer to the specific guidance and training on recording videos, including, but not limited to:
  - Appropriateness of dress
  - Appropriateness of background environment, especially where videos are made away from the School site
  - The data protection and privacy of other people who may appear in the video

In some cases, staff may wish to publish content more widely than the School community. This should be discussed with the Head of Department and/or SLT link first as appropriate. Staff should take care to separate content created on behalf of the School and personal content. This particularly applies where a member of staff may be paid for or receive revenue from such content.

Note that there are already many videos lessons available online for each subject, either linked to our digital textbooks or through other sources, both free and paid. Staff should also consider using these where appropriate.

2 Live Lessons

Live lessons involve staff working with students remotely via the Internet using online meeting software. This is a common tool in business, but is unfamiliar to students and many staff. Therefore, there are particular safeguarding and privacy concerns that need to be addressed.

Live lessons can be very powerful for students when they engage in them. However, not all students can access the Internet at a specific time in order to attend a live lesson, so we must be careful about disadvantaging students who cannot attend live lessons. Similarly, not all staff have the tools and environment to deliver live lessons.

Current expectations around the provision of live lessons are in are COVID-19 documents.

Where staff think it would be useful to deliver a live lesson, they should observe the following:

- The majority of live lessons should be delivered via Google Meet *from within* Google Classroom, as this is the most accessible for students and meets our data protection requirements
  - MS Teams may also be used
  - **Other products must not be used** until they have been approved by the DPO, IT and E-Learning Teams
- Staff must ensure that they have read and understood the most recent guidance, provided by the School, for the platform they wish to use.
  - The guidance may change rapidly, as software is updated and national guidance changes. Changes will be emailed to all staff and communicated via the weekly staff briefing.
- Staff must ensure that their safeguarding, data protection and e-safety training is up to date.
- Live lessons should follow our existing policies, including the behaviour policy, and staff should report any concerns following a live lesson to their HoD, DSL or DPO as appropriate.
- Staff should ensure that students are familiar with the most recent advice provide by the School for live lessons, including, but not limited to:
  - Appropriateness of dress
  - Appropriateness of background environment
  - The privacy of other people who may appear in the video
  - Appropriate online behaviour
- For safeguarding purposes, lessons should either
  - Contain two members of staff or
  - Be recorded
    - Recordings should be stored in Google Drive and **deleted after one year**
    - We do not believe we need additional consent to record the lesson for safeguarding purposes, i.e. where the recording will not be shared. However, it is good practice remind students that the lesson will be recorded
- We recommend that all live lessons are recorded so that they can be shared with members of the class who could not attend the live lesson
  - Recordings should be shared with the rest of the class in a way that is only accessible to that class, e.g. via Google Classroom
  - We do not believe that we need additional consent to share a recorded lesson with the rest of the class, as those class members could have attended the live lesson

    - Students may choose to interact differently if the lesson is recorded, so staff should inform students if the lesson is being recorded and discuss any concerns before the lesson. In some cases, having two staff present and not recording the lesson may be more effective.
- If staff wish to share a recording of a lesson more widely, for example with another class, then this requires the explicit consent of all the students present
    - This should be captured in the recording, by asking students to confirm their acceptance after the recording has started, for example via the chat feature
    - **This must be opt-in, not opt-out**
    - Students must understand how this recording may be used in the future

3 Training

Annual training will be provided to staff on remote learning as part of the annual training on safeguarding, e-safety, data protection and wellbeing. This will also form part of our induction for new staff.

CPD on remote learning will be available each year for staff who wish to developing their knowledge, understanding and skills in this area. This is hosted on our staff IT CPD site here: https://sites.google.com/edgbarrowschool.co.uk/edgcsitstaffcpd/home

Students will be introduced to our general online tools, including the Google Suite, through IT lessons in KS3. Subject-specific applications will be introduced through the relevant subject lessons.

Students will be taught appropriate habits and behaviours for remote learning through our e-safety and PSE programmes.

4 Review

The general principles in this policy will be reviewed annually. Specific guidance will be created and/or updated in response to national guidance, software changes, local circumstances and the needs of the School.