Acceptable Use of IT Policy

(Pupils)

Embrace Multi Academy Trust strives to maintain and improve good provision and outcomes at each of its member schools. Based upon our shared ethos and our values of wisdom, collaboration, respect, integrity, inclusivity and compassion, we aim to support the learning and development of every person within the trust and our policies are written from this perspective.

Version	Approval Level	Document History	Date	Review Period
V1	Trust Leader	Approved	April 2023	2 Yearly

1. Why have an Acceptable Use of IT Policy?

1.1 An Acceptable Use of IT Policy is about ensuring that pupils of Embrace Multi Academy Trust (Embrace), can use the internet, email and other technologies available at their school in a safe and secure way. The policy also extends to out-of-school facilities, eg equipment; printers and consumables; internet and email; managed learning environments and websites.

1.2 An Acceptable Use Policy also seeks to ensure that pupils are not knowingly subject to identity theft and therefore fraud; that they avoid cyber-bullying; and just as importantly, that they do not become victims of abuse. Certain proxy sites and anonymous proxy sites have been banned, because they put the school network at risk. Help us to help you to keep safe.

1.3 Embrace recognises the importance of ICT in education and the need for pupils to access the computing facilities available within the trust in a safe and secure manner. This policy ensures that pupils, parents/carers and members of staff have a clear understanding of the expectations and guidelines when using trust IT facilities.

1.4 Listed below are the terms of this agreement. All pupils at Embrace schools are expected to use ICT facilities in accordance with these terms. Violation of the terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Policy of the school.

2. Equipment

2.1 Vandalism

2.1.1 Vandalism is defined as any action that harms or damages any equipment or data that is part of the school's ICT facilities and is deemed completely unacceptable. Such vandalism is covered by the Computer Misuse Act 1990 (see Appendix 1 - Glossary). This includes, but is not limited to:

- deliberate damage to computer hardware such as monitors, base units, laptops, tablets, printers, keyboards, mice or other hardware
- change or removal of software
- unauthorised configuration changes
- creating or uploading computer viruses
- deliberate deletion of files.

2.1.2 Such actions reduce the availability and reliability of computer equipment and puts other users' data at risk. In addition, they also lead to an increase in repairs to ICT facilities, which impacts upon every pupil's ability to use them, and incurs costs, which reduce the funds available to improve the ICT facilities that the school has.

2.1.3 Embrace reserves the right to charge a reasonable fee for malicious and deliberate damage. Some indicative costs for replacement of common computer equipment can be found below:

Keyboard	£10.00
Mouse	£10.00
Monitor	£50.00
Computer	Assessed on a case by case basis

2.2 **Use of removable storage media**

2.2.1 Embrace recommends the use of online services (OneDrive, ShowMyHomework, Google Classroom etc) to transfer work to and from school securely. Most schools restrict the use of memory sticks but, where they are permitted, anti-virus will scan the drive to ensure they are safe before use. Please ensure that permitted memory sticks are only used for the transfer of work.

2.3 **Printers and consumables**

2.3.1 Printers are provided across Embrace for use by pupils. Printers should be used sparingly and for educational purposes only. Pupils should take time to check the layout and proof read their work using the 'print preview' facility before printing.

2.3.2 All printer use is recorded and monitored, therefore any pupils deliberately using the printer for non-educational or offensive material will be subject to the behaviour management measures of the school, which include the following:

- consequences;
- a warning;
- email and/or internet facilities removed;
- a letter home to parents/carers;
- loss of access to the print facilities available within the school.

2.3.3 Some schools have printer accounting systems in place to monitor printer use and reduce wastage of consumables. Costs for schools that have this in place can be found below:

School	Pupil Allocation	Black/White	Colour	Top Up
Brockington	70 credits per term	1 credit	10 credits	50p per 50 credits (ParentPay)
Rawlins	£2.00: Yr7 - Yr11 £5.00: Post-16	A4 Single 1p A3 Single 2p	A4 Single 4p A3 Single 7p	Top-ups determined by ICT

2.4 **Data security and retention**

2.4.1 All data stored on Embrace systems are backed up daily. These backups are stored for up to at least two weeks, in line with the trust Information & Records Retention Policy. Full details of the backup procedure will be held by all schools. If pupils accidentally delete a file or folder in their documents area or a shared area, they should inform a relevant member of staff or the relevant IT department immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than two weeks previously.

3. Internet, email and monitoring

3.1 **Content filtering**

3.1.1 Embrace provides internet filtering that is designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material

is filtered. If pupils come across any inappropriate website or content whilst using school ICT equipment, they must report it to a member of staff immediately, or to the appropriate IT team. The use of internet and email is a privilege and inappropriate use will result in that privilege being withdrawn.

3.2 **Acceptable use of the internet**

3.2.1 All internet access is logged and actively monitored. Usage reports can and will be provided to appropriate members of staff upon request.

3.2.2 Use of the internet should be in accordance with the following guidelines. Pupils must:

- only access suitable material – the internet is not be used to download, send, print, display or transmit material that would cause offence or break the law;
- not access internet chat sites - pupils could be placing themselves at risk;
- never give or enter their personal information on a website, especially their home address, mobile number or passwords;
- under no circumstance, access online games websites during lesson times – these may only be used during supervised clubs;
- not download or install software from the internet -this is considered to be vandalism of the school's ICT facilities;
- not use the internet to order goods or services from online, e-commerce or auction sites;
- not subscribe to any newsletter, catalogue or other form of correspondence via the internet;
- not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If pupils wish to use content from websites, they should consider using the copy and paste facility to move it into another application, copyright permitting;
- never deliberately attempt to access unauthorised websites via the use of proxies – this is strictly prohibited and attempting to do so will be treated as a serious attempt to bypass safeguards in place.

3.3 **Email (where applicable)**

3.3.1 Pupils may be provided with an email address by the school, and the expectation is that they will use this facility for legitimate educational and research activity.

3.3.2 During lessons, email should only be used when instructed by a member of staff, and for educational purposes only. Email can be accessed during pupils' social times, but they should carefully follow the guidelines laid out below.

3.3.3 Pupils are expected to use email in a responsible manner. The sending or receiving of messages which contain any material that is considered sexist, racist, unethical, illegal, or likely to cause offence should not take place.

3.3.4 Where email is provided, address lists are limited to recipients within the individual school that the pupil attends (both to staff and pupils).

3.3.5 When sending an email, pupils should remember:

- to be polite - never send or encourage others to send abusive messages;
- to use appropriate language - pupils are representatives of the school on a global public system - what they say and do can be viewed by others, so never swear, use vulgarities or any other inappropriate language;
- not to reveal any personal information about themselves or anyone else, especially home addresses, personal telephone numbers, usernames or passwords - electronic mail is not guaranteed to be private;
- not to download or open file attachments unless they are certain of both the content and the origin;
- that file attachments may contain viruses that may cause loss of data or damage to the school network.

3.3.6 Email is actively monitored and keyword detection may block offensive language or those identified as being potentially related to bullying.

3.4 **Cyber-bullying**

3.4.1 In the event of a cyber-bullying incident, the same procedures will be followed as for all other incidents of poor behaviour (see school's Behaviour Policy).

3.4.2 In all cases, details of the incident and action taken will be recorded.

3.4.3 The prime concern will be the protection of the victim. Action will continue until the issue is satisfactorily resolved and the bullying ceases. Parents/carers will be kept informed of action taken. The action will be reviewed and modified in light of circumstances and whether the bullying continues.

3.4.4 Strategies to support the victims will involve staff and pupils. A variety of approaches will be used to achieve this.

3.4.5 If it is a serious incident, suspension or permanent exclusion may be considered.

3.5 Bullying incidents will be logged and monitored regularly.

4. Monitoring

4.1 All computer use at Embrace is subject to monitoring, including website tracking and keyword logging, by the IT Support & Safeguarding team. This is to quickly and proactively monitor any safeguarding risks, and to ensure that pupils are using the computer facilities in a safe and responsible manner in-line with the school Acceptable Use of IT Policy.

4.2 Where violations are detected a screenshot is captured for investigation by relevant staff.

5. External services

5.1 **Web-email (where applicable)**

5.1.1 Web-email provides pupils with remote access to their email account from home or anywhere with an internet connection. Use of this service is subject to the following guidelines. Use of the facility is closely and actively monitored and any abuse or

misuse will result in the facility being withdrawn and/or other disciplinary action being taken.

5.1.2 Web-email is provided for staff and pupils of Embrace only. Access by any other person is not allowed.

5.1.3 Pupils must never reveal their password to anyone else.

5.1.4 Pupils should remember to treat file attachments with caution. File attachments may contain viruses that may cause loss of data or damage to the computer from which they are working. They must not download or open file attachments unless they are certain of both the content and the origin. Embrace accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service.

5.2 **Online Learning Environments**

5.2.1 Online learning environments (eg Microsoft Teams and Google Classroom) provide a web-based portal allowing users access to personalised learning resources and lesson materials both within the classroom and outside of the school environment. Use of this service should only be in accordance with instructions from subject tutors and in accordance with the following guidelines:

- online learning environments are provided for use of Embrace staff and pupils only. Access by any other party is strictly prohibited;
- pupils must never reveal their password to anyone else or attempt to access the service using another pupil's login details;
- pupils may be enrolled in virtual classrooms where it may be possible to post to the classroom, which is visible to enrolled staff and pupils. It is important that this is used responsibly and posting anything inappropriate (including inappropriate language or cyber-bullying) will be dealt with in line with the school behaviour policy.

5.3 **Social networking and file sharing sites (Facebook, Youtube etc)**

5.3.1 Whilst accessing social networking sites (Facebook etc) is restricted within the school environment, we appreciate a large number of pupils will use this in free-time outside of school. Pupils should bear in mind that including any details about the school they attend on their profile not only introduces a very serious safety risk, but also makes them a representative of the school. As such, we strongly recommend pupils do not post any such details to any social networking sites.

5.3.2 Any behaviour which could bring the school into disrepute may result in computer access being restricted and further disciplinary action being taken.

5.3.3 The uploading of any photos or videos taken within schools grounds or containing images of any member of staff is not allowed under any circumstance.

5.4 **Live lessons**

5.4.1 Embrace may use Microsoft Teams or Google Classrooms / Google Meet to provide live and interactive online learning outside of the traditional classroom environment.

5.4.2 Pupils must ensure this facility is used responsibly and with the same level of respect for staff and other pupils that they would display in the classroom.

5.4.3 Cameras must remain off at all times.

5.4.4 Chat windows are enabled for pupils to ask questions relating to the topic being taught. They must not be used to disrupt learning by using it for any other reason.

5.4.5 If a pupil is found disrupting learning using this platform, access to the service may be revoked.

6. Privacy

6.1 Passwords

6.1.1 Pupils must never share their password with anyone else or ask others for their password.

6.1.2 When choosing a password, pupils should choose a word or phrase that they can easily remember, but not something which can be used to identify them, such as their name or address. Generally, longer passwords are better than short passwords.

6.1.3 If pupils forget their password, inform a member of staff or the IT department immediately.

6.1.4 If pupils believe that someone else may have discovered their password, then they should change it immediately and inform a member of staff.

6.2 Security

6.2.1 Pupils must never attempt to access files or programs that they have not been granted access to. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.

6.2.2 Pupils should report any security concerns immediately to a member of staff

6.2.3 If pupils are identified as a security risk to the school's ICT facilities, they will be denied access to the systems and be subject to disciplinary action.

6.3 Storage and safe transfer of personal data

6.3.1 Embrace holds information on all pupils and in doing so, must follow the requirements of the Data Protection Act (2018) (see Appendix 1 - Glossary). This means that data held about pupils can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available, according to the Data Protection Act (2018).

6.3.2 Embrace will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

7. Service

7.1 Whilst every effort is made to ensure that the systems, both hardware and software, are working correctly, the school will not be responsible for any damages or loss incurred as a

result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or errors or omissions. Use of any information obtained via the school's ICT system is at the user's own risk. Embrace specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

8. Mobile technologies

8.1 Acceptable use of mobile devices

8.1.1 For reasons of safety and security, pupils should not use their mobile phone or any other technology in a manner that is likely to bring the school into disrepute or risk the welfare of a child or young person.

8.1.2 Modern mobile devices have access to features including: picture messaging; mobile access to the internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of mobile phones also means that pupils working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras. If you are sent inappropriate material, eg images, videos etc, this should be reported immediately to a member of staff within the school.

8.1.3 If mobile telephones are brought into school they must be switched off and kept in the location agreed by the school (see below) to ensure they cause no disruption to teaching and learning. The school, its staff and governing board takes no responsibility for loss or theft of any mobile phones or devices which pupils choose to bring into school.

Arnesby	Turned off and handed to the main office for safe keeping at the start of the school day
Brockington	Turned off, in lockers
Croft	Turned off and handed to the main office for safe keeping at the start of the school day
Huncote	Turned off and handed to the main office. *Bringing in mobile phones is* strongly *discouraged.*
Manorfield	Turned off and handed into the class teacher for safe keeping at the start of the school day
Rawlins	Turned off in bag
Sherrier	Turned off and handed into the class teacher for safe keeping at the start of the school day
St Peter's	Year 5/6 – Turned off and handed into the class teacher for safe keeping at the start of the school day Other Years – Phones not to be brought into school
Swinford	Phones not to be brought into school

8.2 **Tablet PCs and notebooks**

8.2.1 As a trust, we appreciate that pupils have increasing access to personal mobile devices which can be beneficial to education. We strongly advise all pupils to leave any high value devices at home as correct and appropriate ICT facilities will be provided to pupils whenever necessary. Any devices which are brought into school must be used appropriately and responsibly, and only when specific permission is agreed with the class teacher or member of staff. The trust, it's staff and governing board takes no responsibility for loss or theft of any tablet PCs and notebooks which pupils choose to bring into school.

9. Staying safe online (inside and outside of the classroom)

9.1 The following section is some additional guidance and recommendations for pupils and parents/carers, to help ensure that pupils stay safe online. It also provides information on what to do if they find anything they feel is inappropriate online.

9.2 **Turning on parental controls**

9.2.1 The big four UK internet providers (BT, Sky, TalkTalk, Virgin Media) have parental controls that can be enabled, limiting the content that can be accessed when using the internet. The UK Safer Internet Centre has put together easy to follow guides on how to turn on these parental controls, which can be accessed by clicking here.

9.3 **Where to find support**

9.3.1 Please find below a range of resources we have collated for further information should you wish to find out more on how to stay safe online.

Website	What they offer
https://www.thinkuknow.co.uk/	National Crime Agency online education portal with a range of useful guidance and advice for parents and pupils alike.
https://www.ceop.police.uk	National Crime Agency website for reporting content online.
https://smartsocial.com/	Fantastic e-safety resource with in-depth looks at some of the most common smartphone apps (including Houseparty, Snapchat, Instagram etc) and the risks associated with them.
https://www.saferinternet.org.uk/	Online safety tips, advice and resources to help children and young people stay safe online.
https://www.childline.org.uk tel: 0800 1111	Advice and tips on staying safe online, as well as how to deal with cyber bullying and much more.

9.4 **Reporting inappropriate material and behaviour**

9.4.1 If pupils or parents/carers come across material online that they feel is inappropriate, or if a child is having conversations online that parents/carers are concerned are of an

inappropriate or grooming nature, it is important that these concerns are reported to the Child Exploitation and Online Protection service at https://www.ceop.police.uk If parents/carers or their child are in immediate danger, they should call 999.

9.4.2 If pupils or parents/carers need to contact a member of the Embrace IT Support Team or want to report any inappropriate content they have found or have been sent online, please use the contact details below:

Arnesby	itsupport@embracemat.org
	office@arnesby.embracemat.org
Brockington	itsupport@brockington.embracemat.org
	pastoral@brockington.embracemat.org
Croft	itsupport@embracemat.org
	admin@croft.embracemat.org
Huncote	itsupport@embracemat.org
	office@huncote.embracemat.org
Manorfield	itsupport@embracemat.org
	office@manorfield.embracemat.org
Rawlins	itsupport@rawlinsacademy.org.uk
	Report to head of year's email address
Sherrier	itsupport@embracemat.org
	office@sherrier.embracemat.org
St Peter's	itsupport@embracemat.org
	office@stpeters.embracemat.org
Swinford	itsupport@embracemat.org
	admin@swinford.embracemat.org

9.5 **Online chat/socialising**

9.5.1 Pupils should follow our guidance for staying safe in online chat, whether communicating through SMS, Snapchat, Instagram, Houseparty, Discord or one of the many other services available:

- only engage (invite to a chat, or join a chat) with individuals personally know;
- never give out personal or identifying information;
- if someone is asking you to do something online that makes you feel uncomfortable then stop and tell an adult immediately. Do not be pressured into doing anything you do not want to;

- remember, even if you think you are chatting in a one-to-one conversation, it could be being recorded.

Appendix 1 - Glossary

Computer Misuse Act (1990)

The Computer Misuse Act makes it an offence for anyone to have:

- unauthorised access to computer material, eg if you find or guess a fellow pupil's password and use it
- unauthorised access to deliberately commit an unlawful act, eg if you guess a fellow pupil's password and access their learning account without permission
- unauthorised changes to computer material, eg if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

Data Protection Act (2018)

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school, including teaching staff, support staff, volunteers and governors.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files, it also applies to electronic files.

The principles of the Act state that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- kept no longer than necessary;
- processed in accordance with data subject's rights;
- secure;
- not transferred to other countries without adequate provision.

RIPA – Regulation of Investigatory Powers Act (2000)

If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications;
- the acquisition and disclosure of data relating to communications;
- the carrying out of surveillance;
- the use of covert human intelligence sources;
- access to electronic data protected by encryption or passwords.

If a request for authorised access is made to the school, we will provide the appropriate access to your ICT records and files.

Appendix 2 - Acceptable Use of IT Policy Summary

The Acceptable Use of IT Policy outlines the behaviour that is deemed acceptable when using the school's ICT resources, and is provided to help pupils use these resources in a safe and secure way. Parents/ carers are asked to read the policy and ensure their child understands the agreement.

Below is a summary of the main issues to discuss with your child:

a. Whilst access to the internet is provided to support lessons, this must be used responsibly. All internet activity is closely monitored and should not be used for any of the following:
    - online chat/messaging;
    - giving out personal information;
    - downloading and installing software or viruses;
    - any of the above activity, in addition to anything else which is deemed an unacceptable use of the school computers, will be reported to the relevant member of staff and dealt with appropriately.

b. **All computer use is actively monitored**. Please ensure the facilities are used appropriately at all times, and in line with the Acceptable Use of IT Policy.

c. Pupils are not, under any circumstance, allowed to play online games during lesson time.

d. Email access, where provided, is for use both within and outside the school but must be used appropriately and for school work only. Pupils must always ensure they are polite, use appropriate language and never reveal any personal information about themselves. Pupil email within the school is not considered to be private and is actively monitored. Inappropriate use of the system will be passed to a relevant staff member.

e. Pupils must never upload photos or videos taken within school grounds, or containing images of any members of staff, to online social networking and file sharing websites (such as Facebook, YouTube etc)

f. Pupils must never share their password with anyone else, or ask anyone else for their password. If they forget their password or think someone else may know it, they should speak to a member of staff or the relevant IT department immediately.

g. Pupils must never attempt to access files or programmes to which they have not been granted access by a member of staff.

h. If mobile phones are brought into school, they must be switched off and placed in the appropriate location during the school day.