Marches Academy Trust

Date of last review: **September 2020**
Approved: **30.09.20**
Date of next review: **September 2021**

ICT Policy

www.marchesacademytrust.co.uk

CONTENTS

1. Introduction

This policy will apply to the use of all digital equipment in schools of the Marches Academy Trust and is designed to protect the pupils, staff and resources.

Digital technology is now embedded in the curriculum within the Trust. Technology in a wide variety of forms is used extensively for course work, research, exam entry, lesson delivery, organisation and administration. The Trust digital resources serve community groups, ICT training for teachers, links with other Trusts, email, etc.

We are very aware of the potential problems and issues associated with accessing material available on the internet but see the correct use of internet resources as an essential educational tool in a modern technological society.

Other concerns are the protection of data, security of the network infrastructure, care for the physical equipment, hacking, virus protection and online digital content.

The need for guidelines and rules concerning the use of digital resources in the Trust is clearly recognised and, before being allowed to use digital resources, all users must be prepared to accept and abide by the rules laid down by the Trust.

Access to the internet will enable users to explore thousands of libraries, databases and bulletin boards whilst exchanging messages with other internet users throughout the world. However, some materials, accessible via the internet, may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst we take every precaution to prevent such access, we cannot absolutely guarantee it. We believe strongly that the benefits to pupils from access to the internet, in the form of information resources and opportunities for collaboration, exceed the disadvantages.

Staff will give users guidance on how to access the internet sites effectively and in so doing guide users towards appropriate materials but sanctions will be applied to users who do not follow the guidelines and rules laid down by the Trust.

Outside school, we can only warn of the dangers of the internet and advise suitable monitoring of its use, especially for pupils who attend the schools within the Trust. Parents/carers are advised to monitor closely social networking sites, text messaging and email communications accessed by their children out of school. If any user believes that there has been a communication that breaches any legislation or puts a child or member of the Trust at risk they should report it to the headteacher, safeguarding lead or police immediately.

2. General considerations

2.1 Effective use of the internet

- Use of the internet in school should be a planned activity with clear objectives, with information about suitable sites for researching a topic being made available.
- The effective use of search engines should be taught as part of the planned activity, to reduce the wasting of time and limited resources.
- Saving internet data to user directories should be taught as part of the planned activity, especially picture files and text.
- Copying, pasting and inserting internet data into Word, Excel, Publisher, etc should be encouraged – for further editing and improved presentation.

- Lists of useful website addresses should be kept in user-created Word documents, which can then be used as a set of hyperlinks.
- The use of the internet must be closely monitored at all times by staff at school or by parents/carers at home; this may also be via digital devices such as mobile phones, tablet devices, iPads etc.

2.2 Location access

Adequate consideration should be given to the physical security of rooms containing sensitive information and ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

2.3 Equipment siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved.
- Equipment should be sited to avoid environmental damage from causes such as dust and heat.
- Users should avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users.
- A ‘clear desk policy’, ie hard copies of sensitive data are not left unattended on desks.
- Users should be aware of the dangers of sending out sensitive data and should use encryption or restricted user access on shared files and school/trust systems.
- Staff should not use interactive whiteboards or displays visible to pupils for the purpose of viewing emails

The same rules apply to digital activity on any Trust systems or equipment in use away from school or at a user’s home.

2.4 Private hardware and software

Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the Trust’s equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use by staff of all private hardware and software for Trust purposes must be approved by line managers.

2.5 Disposal of waste

Disposal of waste ICT media will be made with due regard to the sensitivity of the information it contains. For example, paper will be shredded if any confidential information from it could be derived.

The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

2.6 Disposal of equipment

Prior to the transfer or disposal of any ICT equipment the IT team will ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act 2018 to be met.

It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

2.7 Repair of equipment

If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from the hard drive and saved in a secure location for subsequent reinstallation.

The Trust will ensure that third parties are currently registered under the Data Protection Act 2018 as personnel authorised to see data and as such are bound by the same rules as Trust staff in relation to not divulging the data or making any unauthorised use of it, but this needs to be confirmed before the equipment is made available for repair.

2.8 Photographs and video

It is important to gain consent from parents/carers if videos or photos of pupils are going to be used in publications, social media, websites or any shared digital format. If photos/video are going to be used online then names of pupils should not be directly linked to the image.

Staff must be fully aware of the consent form responses from parents/carers when considering use of images; where possible a further request for permission should be acquired, particularly in public facing publications and digital presentations.

Where possible staff should only use school cameras and devices to capture images and should avoid using personal devices.

Parents/carers are permitted to take images of their own children in Trust events. They should not share photos/videos from Trust events on social networking sites if other pupils appear in the image.

Pupils should not take pictures or video of other pupils or staff other than in a controlled supervised educational context where permission has been obtained in advance.

3. Digital technology use

3.1 Mobile phones and other devices

Primary age pupils are not permitted to use **mobile phones** in school or on school activities. Primary age pupils may access other approved digital devices as determined by the school.

Pupils must use all digital devices considerately and responsibly at all times.

For the purpose of this policy, permitted digital devices include notebooks and laptops and any other similar electronic equipment including their data storage media.

Whilst the Trustees give permission for permitted devices to be brought to school, responsibility for the device rests with the pupil and the Trust will take no financial responsibility for loss. **The Trust bears no responsibility for confiscated items.**

Devices are only permitted for use inside lessons under the control and instruction of the class teacher. Unless a teacher has given permission for devices to be used as an integral part of the learning they are not permitted to be seen in school and may not be carried on a pupil's person. All devices must be switched off at all times in the bottom of the bag.

During lessons, devices must be switched off and kept in bags out of sight unless instructed otherwise by the class teacher.

Staff will decide when it is appropriate to use digital devices and will state this in their lessons. Refusal to comply with a teacher will result in the behaviour policy being applied.

Devices are not permitted to be used outside lessons at any time.

3.1.1 During lessons, permitted devices must be switched off and kept in bags out of sight unless instructed otherwise by the class teacher.

3.1.2 Appropriate use of permitted devices in a school library or learning resource centre are confined to learning purposes. Permission to use a device will need to be sought from a member of staff.

If devices are used incorrectly, pupils will be challenged; devices will be confiscated, and retained centrally. Parents/carers will be asked to collect the device directly before 4pm, or send their child with a letter for its return, which will be directly to the pupil after 3pm on the day that a letter is received.

The schools in the Trust reserve the right to decide what is deemed as unacceptable use of any device.

3.1.3 Pupils must ensure that files stored on devices do not contain violent, degrading, pornographic images, or images of staff or other pupils taken without their permission. Use of a device for any negative purpose will not be accepted. The transmission of some information is a criminal offence.

3.1.4 Cyber-bullying is completely unacceptable and is taught as such during ICT and Citizenship lesson for all pupils. If proven this will result in the behaviour policy being invoked, and could lead to fixed term or permanent exclusion.

Senior members of staff may need to view data stored on devices if there is due cause to suspect that these conditions have been broken. Pupils found to be responsible for an offence will have their device confiscated; it will be returned to their parent/carer, or passed to the police. **If there is suspicion that a device contains inappropriate images or digital content involving a minor it will not be interrogated but it will be confiscated, and the device will be passed on to the police for investigation.**

3.1.5 Digital devices must not be used by pupils to call emergency services or to contact parents/carers, when they are feeling unwell. If there is an incident which requires emergency services, pupils must speak to a member of staff who will deal with the matter following the normal Trust policy. All contact with parents/carers to arrange the collection of pupils from Trust must be made by staff in the normal way.

Parents/carers should not contact pupils during lessons. In an emergency parents/carers should phone reception and a message will be taken to the student.

It is not appropriate for pupils to use devices to contact home regarding incidents that occur during the school day. Parents/carers receiving such calls should allow time for details relating to any incidents to be gathered in the usual way and for a member of staff to contact them should this be necessary.

3.1.6 Digital devices, including mobile phones, cannot under any circumstances be taken into examination rooms. Breach of this rule will lead to invalidation of that examination and potentially other examinations.

3.1.7 Pupils need to acknowledge that it is a privilege to bring permitted digital devices to school and abuse of this policy may lead to a curtailment of this privilege.

3.1.8 Pupils who do not sign up to this policy are not permitted to bring any digital devices whatsoever into school. Consequences for failing to adhere to any part of this policy can include permanent exclusion.

3.2 Passwords

Passwords should be changed regularly. Pupils and staff should not share passwords and staff must never let pupils use their login details or account. Staff must ensure that systems are not left logged on unattended; the system may be 'locked' for short periods.

3.3 eSafety in the curriculum

We believe it is essential for eSafety guidance to be given to pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- Schools in the Trust have a framework for teaching internet skills in ICT lessons.
- Schools will provide regular bulletins to parents/carers to proactively engage pupils, parents/carers in avoiding the dangers of popular social media sites
- Educating pupils on the dangers of technologies that maybe encountered outside school is done in ICT lessons and through assemblies.
- 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 in Key Stage 3 about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; ie parent/ carer, teacher/trusted staff member, or an organisation such as Childline.
- Pupils actively participate in the annual Safer Internet Days.

4. Communication

4.1 Use of email and social networking

Communication between pupils and staff should only be through use of email addresses that have been issued by the schools in the Trust (see also 4.2 below). The email system should only be used for school related matters and only used in a way that supports the efficient running of the school. Pupils and staff are advised to maintain an alternative personal email address for use at home in non-school related matters. **Parents/carers are cautioned to monitor closely such personal use of all digital communication devices.**

Pupils are not permitted to use social networking sites within school with the exception of sixth form pupils studying courses with an emphasis on social media.

In the use of email communication, including any forwarding of a third party email, or the use of a social networking site, staff must not act in way that could be considered a breach of their terms and conditions of employment, including in relation to honesty and loyalty to the Trust, or a breach of the Trust's code of conduct for staff or associated guidance issued to staff. Teaching staff have the additional requirement to ensure that at all times their conduct reflects that expected by the Teachers' Standards – Part 2 Personal and Professional Conduct.

To uphold this expectation staff must have particular regard for the following:

- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school/Trust events without the Headteacher's consent.
- Staff must not use social networking sites within lessons unless they are approved by the Trust.
- Staff must not post or share photographic images or caricatures of any member of the Trust community, on any social networking or communication system, without the permission of the individual(s) displayed.
- Staff must not send, or forward, any email containing language or images which could be considered to be abusive, indecent and/or offensive.
- Staff must not send, or forward, any email or emails with content which present grounds for their action to be considered as 'harassment' or 'bullying' as defined under the Trust's harassment and bullying policy and procedures.
- Staff must not send, or forward, any email which would represent an inappropriate disclosure of personal and/or confidential information.
- Staff must not knowingly send, or forward, any email which contains inaccurate, defamatory or libellous statements.

For security purposes staff should also have regard to the following:

- Staff should review and adjust their personal privacy settings to give them the appropriate level of privacy.
- Staff should not turn off any security system which has been put in place by the Trust.
- Staff should not respond to any spam emails or click on any links within such emails. Any received spam or phishing emails should be reported to the network management staff.
- Staff should be wary when receiving an unsolicited email where the sender is unknown. Any email which would appear to have no legitimate purpose should be deleted without being opened.
- Staff should not provide personal information to any email sender or website that is not known to them and/or not trusted.

The provisions of this policy are underpinned by the requirement for staff to sign and adhere to the Appropriate Use Policy at Appendix 2. Conduct by staff which would be considered a breach of the Trust's policy may lead to action under the Trust's disciplinary procedure. Staff should report any concern/evidence that a colleague has acted in a way as to breach the policy.

This policy does recognise that there may be occasions when a member of staff may have a legitimate need to forward an email communication with content of concern, reflected in the provisions above, for the purpose of reporting the matter to senior management.

4.2 Staff Communication

Both for the purpose of maintaining confidentiality and security and also upholding the Trust's Guidance for Safe Working Practice in relation to the need to maintain professional boundaries staff should only communicate with pupils and parents/carers through official channels. These channels include:

- post on Trust headed paper;
- Trust telephone system;
- Trust provided mobile phone;
- Trust email system;
- Trust provided video conferencing equipment.

Staff should not use personal communication devices or systems to contact pupils or parents/carers.

Failure to comply with this requirement without good cause or reason may lead to action under the Trust's disciplinary procedure.

5. Guidelines and restrictions

5.1 Staff and pupil guidelines for using the internet and digital resources

5.1.1 Users are responsible for good behaviour on the internet, as would be expected in any teaching/learning situation.

5.1.2 The internet is provided for users to conduct research and communicate with others, and all users must be prepared to accept and abide by the rules laid down by the Trust.

5.1.3 Access to the internet in school is a privilege, not a right and this privilege can be removed if irresponsible behaviour is suspected.

5.1.4 Individual users of the Trust network and internet are responsible for their communications and this presumes that users will use the system sensibly. Files stored in any digital form such as on: the server, disks, data cards, within email accounts, stored on virtual drives or online may not be kept totally private, especially if it is suspected that their content is illegal or offensive in any way. Emails and other digital tools will be monitored or read electronically to check for offensive content or attached files and may be passed to the police if it is thought an offence may have been carried out.

5.1.5 During Trust-based digital content lessons and internet access time, staff will guide users towards the use of appropriate materials, but away from school, parents/carers have the responsibility for guidance and use of the internet, social networking sites, text messaging, email and other digital communication accessed by their children. If any negative use of social networking carries over into the Trust context linked with any Trust stakeholder – the Trust will take any necessary disciplinary action.

5.1.6 Data of a personal nature stored on any digital device that is taken off-site must be password protected or encrypted. Where data is covered under the Data Protection Act, the

Trust’s Data Protection Policy should be referred to. Staff are discouraged from taking any personal data off-site in digital form as loss or misuse of the data will be taken seriously and disciplinary action will follow if appropriate steps have not been taken to secure it.

5.2 Restrictions

The following are **not** permitted on or through any digital resource; anything that contravenes these will be taken seriously for both pupils and staff. Normal disciplinary procedures will apply:

5.2.1 Sending, storing or displaying illegal or offensive messages or pictures.

5.2.2 Using offensive, unacceptable or obscene language.

5.2.3 Harassing, insulting or attacking others over the internet, via social networking or using any digital medium.

5.2.4 Damaging computers, computer systems or computer networks including all software and hardware.

5.2.5 Changing set-ups on the Trust computers, workstations, servers or digital tools.

5.2.6 Violating laws such as: copyright designs and patents, data protection legislation, child protection guidance, computer misuse act and any law that covers digital communication or use.

5.2.7 Using others’ user names, passwords and accounts.

5.2.8 Trespassing in other users’ or administrative folders, files or work.

5.2.9 Intentionally wasting resources.

5.2.10 The use of the internet for personal and business other than in connection with the business of the Trust.

5.2.11 Making, distributing or using unlicensed software or data.

5.2.12 Infecting digital media with software viruses intentionally or through negligence.

5.2.13 Photos or video from Trust events or of Trust pupils should not be placed on any social networking sites, publications or digital presentations without the written consent of the child and their legal guardian.

5.3 Monitoring

Monitoring of in school e-safety incidents takes place and records are kept. The records are reviewed/audited and reported to the Trust’s senior leaders. Parents/carers are informed of e-safety incidents, as relevant.

The impact of the ICT policy and practice is monitored through the audit of e-safety incident logs and behaviour / bullying logs.

6. Sanctions

Whilst every effort will be made to establish fault or accountability, suspicion will be enough to enforce the following.
For Pupils

Level 1 - What will happen if any user contravenes any of the above rules

The users' school account and access to digital devices/accounts will be stopped.

An initial investigation will be carried out after which the account will be re-enabled, escalated to the second level or in an extreme case, taken to the third level of sanction depending on the findings.

The pupil will be warned and a communication will be made with parents.

At secondary age, an after-school detention will be given.

Level 2 - What will happen if any user repeats the offence, contravenes a second rule or it is deemed that the first offence was more serious

Access to network accounts and digital devices will be disabled for **two weeks**.

The pupil's parents/carers will be informed by telephone and via a written communication.

Staff will be informed that the account has been disabled.

At secondary level, an after-school detention will be given.

Level 3 - What will happen if any Trust network user continues to contravene the above rules or it is deemed that the first or second offence was more serious

A fixed term exclusion will be imposed.

Return to school will be allowed following a contract meeting with parents/carers.

What will happen if any Trust network user persists in violating the rules for use of digital resources or where the offence is considered more serious or impacts on other Trust policies

These cases will be referred to the Leadership Group and network accounts may be closed or disabled for two terms or longer. **The governors will consider very serious cases of misuse of digital technology at the Trust and this may lead to further exclusion, expulsion and matters being reported to the police.**

For Staff

Network management staff are allowed to check **all** digital tools, network accounts, virtual learning accounts, staff laptops, staff work stations and internet based facilities for content, so that they can effectively assist with control and monitoring of internet access and use of digital resources and communications. The network management staff are subject to these *User Guidelines* when accessing digital resources for their own purposes. In the event that it is suspected that there are illegal or offensive images or digital content involving a minor, images will not be viewed but will be passed to the police for investigation.

Staff are cautioned that use of Trust digital resources from home are subject to the same monitoring and control as use in Trust.

A member of staff who breaches any of the restrictions within this policy for users of school/trust digital resources will be dealt with in line with the law, DfE guidance and school/trust policies. Serious cases will follow disciplinary procedures and could lead to criminal prosecution.

All staff and pupils are required to sign the Trust's acceptable use policy agreement (Appendices 1 and 2).

Appendix 1 - ICT appropriate use policy for pupils

The policy aims to ensure that any digital communications technology is used without creating unnecessary risk to others.

I agree that I will:

- only use, move and share personal data securely;
- respect the Trust network security;
- set strong passwords which I will not share;
- not use my own mobile device in school unless I am given permission;
- respect copyright and the intellectual property rights of others;
- only create and share content that is legal;
- always follow the terms and conditions when using a site;
- only visit sites which are appropriate;
- discuss and agree my use of a social networking site with a responsible adult before joining;
- obtain permission from a teacher before I order online;
- only use approved email accounts;
- only use appropriate content which I have permission to use;
- only communicate online with trusted users;
- never meet an online friend without taking a responsible adult that I know with me;
- make sure all messages/posts I send are respectful;
- not respond to or forward any inappropriate message or content;
- be cautious when sharing personal contact information;
- only communicate electronically with people I know or have been approved by my school;
- report unsuitable content or activities to a member of staff.

I know that anything I share online, store digitally or use on a digital device may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

CEOP REPORT
ceop.police.uk

I am aware of the CEOP report button and know when to use it.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts;
- breach any Local Authority/Trust policies eg gambling;
- forward chain letters;
- breach copyright law;
- do anything which exposes others to danger.

I accept that my use of the Trust ICT facilities and <u>any</u> digital device used in connection with the Trust or Trust members may be monitored and the outcomes of the monitoring may be used.

Pupil name:

Signed:

Appendix 2 - Appropriate use policy for any adult working with learners

The policy aims to ensure that any digital communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely;
- respect the Trust network security;
- implement the Trusts policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources;
- respect the copyright and intellectual property rights of others;
- only use approved email accounts;
- only use student images or work when approved by parents/carers and in a way that will not enable individual pupils to be identified on a public-facing site;
- only give permission to pupils to communicate online with trusted users;
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues;
- not use or share my personal (home) accounts/data (eg Facebook, email, eBay etc.) with pupils;
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs);
- report unsuitable content and/or ICT misuse to the named e-Safety officer;
- promote any supplied e-Safety guidance appropriately;
- when I use my personal hand held / external devices (PDAs/laptops/mobile phones/USB devices etc) in school, follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

I know that anything I share online, store digitally or use on a digital device may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I understand that the Trust will monitor my use of the ICT systems, email and other digital communications.

I understand that the rules set out in this agreement also apply to use of Trust ICT systems (eg laptops, tablets, email, cloud services) out of school.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - inappropriate images
    - promoting discrimination of any kind
    - promoting violence or bullying
    - promoting racial or religious hatred
    - promoting illegal acts

    - breach any Local Authority/Trust policies eg gambling;
- do anything which exposes others to danger;
- post any other information which may be offensive to others;
- forward chain letters;
- breach copyright law;
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission;
- store images or other files off site without permission from the Headteacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that the Trust's data protection policy requires me to keep any information I see regarding staff or pupils, which is held within the Trust's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school/Trust ICT systems (both in and out of school) and my own devices (in Trust and when carrying out communications related to the Trust) within these guidelines.

Staff/Volunteer name:

Signed:

Appendix 3 - Appropriate use policy guidance notes for Trustees and Governors

The policy aims to ensure that any digital communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

Trustees/Governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning;
- learners are made aware of risks and processes for safe digital use;
- all adults and learners have received the appropriate acceptable use policies and any required training;
- the Trust has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety;
- an e-Safety Policy has been written by the Trust, building on the LSCB e Safety Policy and BECTA guidance;
- the e-Safety Policy and its implementation will be reviewed annually;
- the Trust internet access is designed for educational use and will include appropriate filtering and monitoring;
- copyright law is not breached;
- learners are taught to evaluate digital materials appropriately;
- parents/carers are aware of the acceptable use policy;
- parents/carers will be informed that all technology usage may be subject to monitoring, including Universal Resource Locator’s and text;
- the Trust will take all reasonable precautions to ensure that users access only appropriate material;
- the Trust will audit use of technology establish if the e-safety policy is adequate and appropriately implemented;
- methods to identify, assess and minimise risks will be reviewed annually;
- complaints of internet misuse will be dealt with by a senior member of staff.

Appendix 4 - Parent letter – digital technology / internet / email use

The Trust

Parent/carer name:
Pupil name:
Pupil's registration class:

As the parent or legal carer of the above pupil(s), I grant permission for my child to have access to use the internet, the Virtual Learning Environment, Trust email and other ICT facilities at Trust. I know that my daughter or son has signed a form to confirm that they will keep to the Trust's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the Trust cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the Trust will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the Trust can check my child's computer files, digital devices, email, social networking sites and the internet sites they visit. I also know that the Trust may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the Trust by promoting safe use of the internet and digital technology at home and will inform the Trust if I have any concerns over my child's e-safety.

I am aware that the Trust permits parents/carers to take photographs and videos of their own children in Trust events and that the Trust requests that photos/videos are not shared on any personal social networking site such as Facebook if the photos/videos contain images of other children. I will support the Trust's approach to eSafety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the Trust community.

The full ICT policy is available on the Trust website and was attached to this letter. I accept the principles of this policy and the restrictions and consequences it outlines.

Parent/carer's signature:

Date: