Acceptable Use of the Internet and IT Systems Policy

Policy Code:	IT1
Policy Start Date:	April 2021
Policy Review Date:	April 2023

Statement of intent

Whilst our Trust promotes the use of technology and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the relevant headteacher or Trust IT Lead in order for any necessary further action to be taken.

This Acceptable Use of the Internet and IT Systems Policy is also designed to outline staff responsibilities when using technology, whether this is via personal devices or school/Trust devices, or on/off the Trust's premises, and applies to all staff, volunteers, contractors and visitors.

1. Introduction

1.1 This policy applies to all employees, volunteers, supply staff and contractors using CIT ICT facilities.

1.2 Pupils may also be required to sign the 'Technology acceptable use agreement' for their respective school (if age and ability appropriate). All pupils will complete e-safety lessons where the schools' acceptable use protocols will be explained in an age appropriate way.

1.3 The school Acceptable Use Policy is divided into the following three sections.

- General Policy and Code of Practice;
- Internet Policy and Code of Practice;
- Email Policy and Code of Practice.

1.4 This policy should be read in conjunction with the Trust's Data Protection Policy and Privacy Notices.

2. General Policy and Code of Practice

2.1 The Trust has well-developed and advanced ICT systems, which it intends for you to benefit from.

2.2 This policy sets out the rules that you must comply with to ensure that the system works effectively for everyone.

Privacy

2.3 The 'UK GDPR' and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the Trust stores on its network regarding staff, pupils and other natural persons it deals with whilst carrying out its functions.

2.4 The Trust will only process data in line with its lawful basis to uphold the rights of both pupils and staff and other third parties.

2.5 In order to protect pupils' safety and wellbeing, and to protect the Trust from any third party claims or legal action against it, the Trust may view any data, information or material on the its ICT systems (whether contained in an email, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the Police or Social Services. The Trust's privacy notice details the lawful basis under which the Trust is lawfully allowed to do so.

Code of Practice

The Trust's philosophy	In using ICT, you will follow the Trust's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods.
User ID and password and logging on	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be changed from the default password when the account was set up. If you forget or accidentally disclose your password to anyone else, you must report it immediately to a member of the IT support staff, for example the Lead IT at a the school or Ark IT Engineer. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. Use of the Trust's facilities by a third party using your user name or password will be attributable to you, and you will be held accountable for the misuse. You must not log on to more than one computer at the same time.
Printing	The Trust may wish to check that expensive resources are being used efficiently and the member of staff may suggest other strategies to you to save on resources.
Logging off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving. Staff should operate a clear screen, clear desk approach and not leave anything confidential on their screen or desk when they leave.
Access to information not normally available	You must not use the system or the Internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the system	You must not connect any hardware which may be detrimental to the Trust's networks.

Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff. You must never attempt to use any of the connectors on the back of any desktop computer. USB memory sticks have been disabled as a security measure as are other portable storage media. You are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.
Virus	If you suspect that your computer has a virus, you must report it to a member of the ICT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the Trust's system.
File space	You must manage your own file space by deleting old data rigorously and by deleting emails that you no longer require. If you believe that you have a real need for additional space, please discuss this with the Trust's IT Lead or relevant Ark engineer.
Transferring files	You may transfer files to and from your network home directories using the Cloud apps set up in Microsoft Office 365. When transferring files to and from your network home directories, you must not import or export any material unless the owner of that material expressly permits you to do so.
Reporting faults and malfunctions	You must report any faults or malfunctions in writing to the ICT support staff, including full details and all error messages, as soon as possible.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, into the ICT rooms. You must always maintain a clean and quiet working environment.
Copying and plagiarising	You must not plagiarise or copy any material which does not belong to you.
Copies of important work	All data across the Trust's network is backed up. Should you lose any information please contact the IT staff immediately to recover the information. Any data containing personal and special category data must not be stored on general access drives. They should be stored in specific folder that have the correct permissions set up on. This can be done via the IT support staff.

3. Internet Policy and Code of Practice

3.1 The Trust can provide access to the Internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.

3.2 Whenever accessing the Internet using the Trust's or personal equipment you must observe the Code of Practice below.

3.3 This Policy and Code of Practice are designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the school's facilities and information being damaged.

3.4 Any breach of this Policy and the Code of Practice will be treated extremely seriously, and it may result in disciplinary or legal action or expulsion.

3.5 The Trust may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this Policy and Code of Practice.

Why is Internet access available?

3.6 The Internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which would be useful for educational purposes.

Why is a Code of Practice necessary?

There are four main issues:

1. Although the Internet is often described as 'free', there is a significant cost to the Trust for using it. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support Internet access.

2. Although there is much useful information on the Internet, there is a great deal more material which is misleading or irrelevant. Using the Internet effectively requires training and self-discipline. Training is available on request from ICT staff.

3. Unfortunately, the Internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect the staff and pupils who access to the Internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.

4. There is a danger of importing viruses on to the Trust's networks, or passing viruses to a third party, via material downloaded from or received via the Internet, or brought into the Trust and its schools on disks or other storage media.

Code of Practice

Use of the Internet	The school/Trust Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use. You may use the Internet for other purposes provided that: • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties; and • You always follow the Code of Practice.
Inappropriate material	You must not use the Internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by pupils. You are responsible for rejecting any links to such material which may appear inadvertently during research. All sites across CIT have strict Internet filtering in place, but it is impossible to filter out every inappropriate website. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform the ICT support staff immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The Internet access system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
Giving out information	You must not give any information concerning the Trust, its schools, its pupils or parents, or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the Trust or school's name and your name when accessing a service which the school subscribes to.
Personal safety	You should take care with who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the Internet.
Hardware and software	You must not make any changes to any of the Trust's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the Trust/school are an important part of the Trust's security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage systems.

Copyright	You should assume that all material on the Internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the Internet unless the owner of the website expressly permits you to do so.

4. E-mail Policy and Code of Practice

4.1 The school's computer system enables members of the Trust/schools to communicate by email with any individual or organisation with email facilities throughout the world.

4.2 For the reason outlined above, it is essential that a written policy and Code of Practice exists, which sets out the rules and principles for use of email by all.

4.3 Any breach of this policy and Code of Practice will be treated seriously and it may result in disciplinary or legal action or expulsion.

4.4 The school may take steps, including legal action where appropriate, to recover from an individual any expenses or liabilities the school incurs because of the breach of this policy and Code of Practice.

Code of Practice

Purpose	You should only use the Trust's email system for work related emails. You are only permitted to send a reasonable number of emails.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form). The Headteacher, Trust senior staff and technical staff are entitled to have read-only access to your emails.
Security	As with anything else sent over the Internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents. As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email. CIT does operate an Encryption system if emails of a sensitive nature do need to be sent out. The IT staff can help with this.
Program files and non-business documents	You must not introduce program files or non-business documents from external sources on to the Trust's networks. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100 percent successful, so introducing nonessential software is an unacceptable risk for the school.

	If you have any reason for suspecting that a virus may have entered the Trust/school's system, you must contact the ICT support staff immediately.
Quality	Emails constitute records of the Trust/school and are subject to the same rules, care and checks as other written communications sent by the school. Emails will be checked under the same scrutiny as other written communications. Staff members should consider the following when sending emails: • Whether it is appropriate for material to be sent to third parties; • The emails sent and received may have to be disclosed in legal proceedings; • The emails sent and received maybe have to be disclosed as part of fulfilling an SAR; • Whether any authorisation is required before sending; • Printed copies of emails should be retained in the same way as other correspondence, e.g. letter; • The confidentiality between sender and recipient; • Transmitting the work of other people, without their permission, may infringe copyright laws; • The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken; • Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by email about yourself, other members of staff, pupils or other members of the school community. If you receive any inappropriate emails or attachments you must report them to technical staff.
Viruses	If you suspect that an email has a virus attached to it, you must inform the technical staff immediately.
Spam	You must not send spam (sending the same message to multiple email addresses) without the permission of senior staff.
Storage	Old emails may be deleted from the Trust/school's server after 12 months. You are advised to regularly delete material you no longer require and to archive material that you wish to keep.

Message size	Staff are limited to sending messages with attachments which are up to 2Mb in size. If you wish to distribute files within the Trust/school, you can do so by using shared areas.
Confidential Emails	You must ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.

5. E-mail policy – advice to staff

5.1 Staff should remind themselves of the ICT Acceptable Use Policy which relates to the monitoring, security and quality of emails. In addition, staff should be guided by the following good practice:

- Staff should check their emails daily and respond, as appropriate, within a reasonable period if the email is directly addressed to them;
- Staff should avoid spam, as outlined in this policy;
- Staff should avoid using the email system as a message board and thus avoid sending trivial global messages;
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters;
- Whilst accepting the convenience of the staff distribution list, staff should try to restrict its use to important or urgent matters;
- Staff should send emails to the minimum number of recipients;
- Staff are advised to create their own distribution lists, as convenient and appropriate;
- Staff should always include a subject line;
- Staff are advised to keep old emails for the minimum time necessary.

6. Further guidance

- Remember – emails remain a written record and can be forwarded to others or printed for formal use;
- As a rule of thumb, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion;
- Remember, “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression;
- Remember that sending emails from your school account is similar to sending a letter on school letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school;
- Linked with this and given the popularity and simplicity for recording both visual and audio material, staff are advised to remember the possibility of being recorded in all that they say or do.

For further information or to clarify any of the points raised in this policy please speak to the Lead IT/DPO.

The Community Inclusive Trust

Acceptable Use of the Internet and IT Systems Policy

This Policy has been approved by the Executive Leadership Team

Signed…… Name..... Date:

Chair of the Trust Board

Signed…… Name..... Date:

Chief Executive Officer