BEACON EDUCATION

AMBITION RESPECT EXCELLENCE

ICT Acceptable Use Policy

Document Title	ICT Acceptable Use Policy		
Version Number	1		
Status	Draft		
Publication Date	01/12/2022		
Statement Owner/Author	Tony Ayre		
Related Policies/Procedures	Online Safety Policy		
Review Date	01/12/2023		
Approved/Ratified by	CEO	**Date:**	December 2022
Distribution	All users		

STAFF AND VOLUNTEER ACCEPTABLE USE POLICY

Trust Policy

This Acceptable Use Policy reflects the Trust Online Safety policy and procedures. The Trust will ensure that staff and volunteers will have good access to ICT to enable efficient and effective working, to enhance learning opportunities for children and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) policy applies to staff, volunteers and guests who have access to and are users of Trust ICT systems and to Trust related use of ICT systems outside of Trust.

My Responsibilities

I agree to:

- read, understand, sign and act in accordance with the Trust Trust Online Safety policy and procedures
- report any suspected misuse or concerns about online safety to the Online Safety Lead
- monitor ICT activity in lessons, extracurricular and extended Trust activities
- model the safe use ICT
- refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the Trust or may bring the Trust into disrepute (this includes personal sites and social media posts)

Education

- I understand that I am responsible for the online safety education of children
- I will respect copyright and educate the children to respect it as well

Training

- I understand that I will participate in online safety training
- I understand that it is my responsibility to request training if I identify gaps in my abilities

Cyberbullying

- I understand that the school has a zero tolerance of bullying. In this context cyberbullying is no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with Trust procedures

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the Trust. These measures include:

- the proxy or firewall settings of the Trust network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)

- Accounts
  - I will only use the user account(s) issued to me by the IT support team, system administrators or designated personnel
  - I will never log another user onto the system using my account
  - I will never log on to the system using another user's account
- Filtering
  - I will not try to bypass the filtering system used by the Trust
  - If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
  - I will report any filtering issues immediately
- I understand that the Trust will monitor my use of computers and the internet

Data Protection

- I understand my responsibilities towards the Data Protection Act and will ensure the safe keeping of personal data at all times.
- I will ensure that all data subject to the Data Protection Act is stored only on Trust network drives, so as to be backed up regularly
- I will ensure that all data held in personal folders is regularly backed up
- I will read and follow the Trust Data Protection Policy

Use of digital images

I will follow the Trust's policy on using digital images making sure that:

- only those children whose parental permission has been given are published
- I will not use full names to identify people
- I will not use personally owned cameras/camera equipped phones to take digital images of children, unless permission is given by a relevant person (Headteacher, manager, COO, CEO), and the photos are deleted immediately after their being copied off the device to a Trust device

Communication

I will be professional in all my communications and actions when using Trust ICT systems.

Email

- I will use the Trust provided email for all business matters, and not personal email accounts
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programs).
- If sending information subject to the Data Protection Policy, I will ensure that it is encrypted by attaching it to the email in an encrypted document, and will disseminate the password separately (e.g. via phone or postal letter).

Social Media

- I will ask permission before I use social media with children or for other Trust related work
- I will not discuss school or Trust related issues on social media without permission

Personal publishing

- I will follow the Online Safety policy and procedures concerning the personal use of social media

Mobile Phones

- I will not use my personal mobile phone during contact time with children unless it is necessary for me to carry out my job (as defined by the Headteacher, nursery manager, COO or CEO), or it is an emergency
- I will not use my personal mobile phone to contact children or parents, unless it is an emergency, per the Online Safety policy and procedures

Reporting incidents

- I will report any incidents relating to online safety to the Online Safety Lead and/or Trust IT Support team.
- I will make a note of any incidents in accordance with Trust procedures
- I understand that in some cases the police may need to be informed

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when children use ICT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the Trust ICT systems in any way then there are disciplinary procedures that will be followed by the Trust.

I have read and understand the full Trust e-safety policy and agree to use the Trust ICT systems (both whilst on and off Trust premises) and my own devices (whilst on Trust premises and when carrying out communications related to the Trust) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name ______________________________

Signed ______________________________

Date ______________________________

PUPIL ACCEPTABLE COMPUTER AND INTERNET USE POLICY

Technology is a great tool to find information and to communicate with others.

Beacon Education MAT and its schools encourage its appropriate, effective and safe use.

All users of technology in the Trust and its schools must agree to certain rules and will only use the equipment and software as instructed.

My Responsibilities

- I will only use ICT systems in school, including, but not limited to, the internet, email, digital video, mobile technologies, etc., for school purposes.
- I will not download or install software on school technologies unless given permission to by the IT support team
- I will only log on to the school network with my own username and password.
- I will not reveal my passwords to anyone.
- I will only use my school email address and not other email sites while in school.
- I will make sure that all ICT communications with children, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- 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.
- I will not use a mobile phone unless told to by a member of staff.
- I will not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone using the internet or email.
- Images of children and/or staff will only be taken, stored and used for school purposes in line with my teachers' instructions and not be distributed outside the school network.
- I will ensure that my online activity, both in school and outside school, will not cause the Trust, my school, the staff, children or others distress or bring the school into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system or other safety or security systems.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted.

Sanctions

I understand that the Trust and my school will monitor my use of computers and other technology.

I understand that the Trust and my school may investigate incidents that happen outside of school.

I understand that there are regulations in place when children use ICT and that there are sanctions if I do not follow the rules.

PUPIL ACCEPTABLE COMPUTER AND INTERNET USE POLICY AGREEMENT FORM

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the Pupil Acceptable Use Agreement and agree to follow these guidelines when:

- I use the school ICT systems and equipment
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name ____

Signed ____

Class _______________ Date ____________________

PARENT/PUPIL ACCEPTABLE USE POLICY

The Internet offers both educational and social opportunities for our children. Whilst recognising the benefits we must also establish appropriate, effective and safe use of the Internet.

The Internet will be used within school to support children's learning both formally (within taught lessons) and informally (outside taught lessons), at the discretion of a member of staff who will set guidelines and rules for its use. Children will be taught to be critical and discriminating in their use of Internet sites and to maintain a balance between the use of technology and other activities.

Children may have opportunities to communicate with others through blogs, publishing work to online galleries and email. This will only take place in accordance with Beacon Education MAT and its schools' policies and procedures, so their full name will never appear publicly online. Responsible and considerate language will be used at all times when communicating with others.

Please read and discuss these rules with your child and return the signed slip to the school. If you have any concerns or questions, please talk to your child's teacher.

Children will:

- only use the Trust ICT systems for those activities which they have been given permission to use and under the appropriate supervision of a member of staff.
- use the Internet within the Trust to support learning.
- be made aware of what cyber-bullying is and what to do if it happens.
- only use the usernames and passwords they have been given by staff, and will not share these with others.
- only use Trust provided accounts when in school, and won't use personal email accounts etc.
- not download and use material or copy and paste content which is copyright or not covered by the school copyright licenses.
- Not attempt to search for, view, upload or download any material that is likely to be unsuitable in a school or is blocked by the Trust's web filter.
- inform a their teacher if they have accidentally accessed inappropriate content.
- use responsible and considerate language in communicating with others.
- be encouraged to maintain a balance between the use of ICT and other activities.
- be encouraged to discuss their use of the Internet and those sites that are age specific especially social networking sites.
- only use mobile phones when told to by staff.
- be encouraged to talk with their parents or carers about the rules for the safe use of the Internet.
- Be made aware that the Trust and/or school may investigate incidents that happen outside of school but could have an effect on the Trust and/or school.
- not give out their personal details to others or arrange to meet other people unless it is part of an approved school project where a responsible adult will be present.
- understand that these rules are here to keep everyone safe.

Failure to comply with these rules will result in one or more of the following:

- A ban, temporary or permanent, on the use of the Internet within the Trust or school.
- A letter informing parents of the nature and breach of rules.
- Appropriate sanctions and restrictions placed on future access to Trust and/or school facilities.
- Disciplinary action in line with the school's policies.

PARENT/PUPIL ACCEPTABLE USE POLICY RETURN SLIP

The form below must be completed, signed and returned to your child's school for our records.

Use of the Internet may be withheld unless this has been done.

I have read, understood and discussed the Parent/Pupil Acceptable Use Policy with my child and I am happy for my child to experience the Internet use described:

Pupil Name (PLEASE PRINT) ________________________________ Class ________

Signature of Pupil ____________________________ Date ________

Name of Parent or Carer (PLEASE PRINT) ________________________________

Signature of Parent or Carer ____________________________ Date ________

IT MANAGER AND TECHNICIAN ACCEPTABLE USE POLICY EXTENSION

The Trust IT Manager or (or person given similar responsibilities) is placed in an exceptional position of trust. Many of the duties that the CEO expects the IT Manager and Technicians to complete are against the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the IT Manager and Technicians to fulfil their duties.

Areas of concern are that:

- Files may be created, imported or processed by staff and children and stored on the Trust's servers or other storage systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the Trust/school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the Trust and/or school e.g., material that might bring the establishment into disrepute.

- Work created during the Trust's time or on the Trust's equipment or on one's own equipment but for school work, belongs to the school, except otherwise agreed by Trust management.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by the IT Manager and Technicians.

- Through work within the Trust network the IT Manager and Technicians may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The IT Manager and Technicians through specific usernames and passwords have control, (sometimes through remote workstations) to the Trust network. In the past there have been examples where these powers have been abused at various schools in the UK.

Because of these areas of concern the ICT Manager and Technician should:

- be responsible for monitoring the Trust network.

- be given permission to access other user's files.

- protect the users by maintaining the web filter(s) for the Trust.

- monitor the internet use of users within the Trust.

- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the Trust's Online Safet Policy and Procedures, and AUPs.

- make sure that they record all usernames and passwords for all the services they access in a place where the executive leaders in the Trust can access them.

- have their use of the Trust network, internet, and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to Data Protection and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the Trust network and internet connections.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g., never open websites that are suspected of having inappropriate material unless others are present).
- have frequent meetings with their line manger to report on any issues or trends.

As an IT Manager / Technician (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the Chief Operations Officer.

Name: ____

Signed: ____

Senior Member of Staff: ____

Date: ____________________

VISITOR ACCEPTABLE USE POLICY

Visitors should apply certain standards when using computer equipment in schools/nurseries. These standards should include an awareness of Data Protection and Copyright laws.

LOGGING IN

- If you use the Trust's equipment, you will need to request a guest log in.
- If you are using equipment that has been logged in by a member of staff always ensure a member of staff is present. Always lock the machine if they need to leave the room.
- If your service contract (Network/MIS/external support) allows you access to the system through team logins inform the Trust IT Support Team how you will be accessing the system.

WIRELESS ACCESS

- Request permission to use the wireless connection (if available) asking for an authorisation key. You may need to change settings on your device for the connection to work correctly on the network.

INTERNET ACCESS

- The Trust's Internet connections are filtered, so access might be denied to some websites. Seek permission to access sites that are unavailable through the Trust's normal filtering system. This might not be possible as changes to the filter can take some time, and some sites contain inappropriate material so will not be unfiltered.
- You are responsible for the websites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never download and install software or updates onto a Trust device without permission from a member of the Trust IT Support Team.

IF YOU USE YOUR OWN EQUIPMENT:

- Make sure that it has up to date virus protection software installed.
- Ensure that you take care with trailing wires.
- Ensure that it is electrically safe to use – no exposed wires, or components, for example.
- Ensure that you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.
- Ensure that there is no inappropriate material on your device.

DOWNLOADING FILES OR DOCUMENTS

FOR ALL FILES

- Make sure that the USB stick/external hard drive has recently been virus checked.
- Never transfer files unless you have permission.
- Make sure that you clearly state the purpose for transferring these files.
- Check to see if the Trust machine you would like to transfer files from or to is encrypted as it might automatically encrypt your USB stick/hard disc drive.

IF THE FILE CONTAINS SENSITIVE PERSONAL DATA SUCH AS STAFF OR STUDENT INFORMATION

- Get permission for this in writing or by email.
- (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed).

- Use an encrypted memory stick or hard drive.
- Transfer the file only over a secure email connection.

IF YOU TAKE PICTURES, VIDEO OR SOUND FILES THEN CHECK

- That you have permission to capture these files.
- That the staff/children have all given their permission for these images/voices to be used.
- That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

Name ____ Date ________________________