NEWBURY ACADEMY TRUST

ICT User Acceptance Policy

DATE APPROVED: February 2016

DATE FOR REVIEW: February 2018

SIGNED: …… .....

On behalf of the Board of Directors

ICT User Acceptance Policy

Name of school: Newbury Academy Trust

Newbury Academy Trust's computing facilities are provided to enable students to further their education and staff to enhance their professional activities including teaching, research, administration and management. Any breaches of this policy will be treated as a disciplinary matter and dealt with appropriately. Sanctions imposed could results in the right to use the facilities to being withdrawn either temporarily or, in extreme circumstances, permanently. The use of the computer system without permission or purpose not agreed by the Trust could constitute a criminal offence under the Computer Misuse Act 1990.

The Trust may use its right, including by electronic means, to monitor use of the Trust's computer systems, including the monitoring of websites visited, the interception of emails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the Trust's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Where misuse of the system is suspected, the IT Support Team will immediately remove the user's access rights pending further investigation.

Purpose

Effective use of the internet and email is crucial to learning and to the effective running of the Trust. To this end it is important that all staff understand the principles of effective, legal and safe use of ICT within a academy environment.

Policy

The Internet

Internet access and email are available to all permanent staff, students, Governors and Directors at Newbury Academy Trust. Staff and students can connect to appropriate websites from around the world using any of our networked PCs or laptops. These websites should provide advice, guidance and information resources for the benefit of Newbury Academy Trust.

When staff access the internet from work they are representing the Trust and using Trust resources. Staff are responsible for ensuring that the internet is used in an effective, ethical and lawful manner and that the reputation of the Newbury Academy Trust is protected at all times.

Downloads

File downloads from the internet are only permitted for work-related documents e.g. Government reports, strategy documents, academy and college prospectuses. All other downloads are unacceptable unless specifically authorised in writing by IT Support. IT Support is permitted to use the internet to download software updates and patches as required to keep the IT infra-structure maintained. Staff and students must not upload, download or distribute any materials that are or may be interpreted to be

defamatory, abusive or offensive to any other individual or organisation. A claim for defamation, discrimination or harassment may be brought against staff and students and/or Newbury Academy Trust if they do not comply with this provision.

Email

All permanent and temporary staff, Governors and Directors are provided with their own Openhive email account through Capita. Staff should not use "web based" email services, such as Hotmail, Yahoo Mail etc. using Newbury Academy Trust equipment, unless specifically authorised to do so.

Staff should be aware that deletion of a message or file will not fully eliminate it from the computer system. Email should not be used as a "chat line."

Staff should regularly delete old email messages to avoid filling up storage space. When staff use the email system they are representing the Trust. They are responsible for ensuring that email is used in an effective, ethical and lawful manner and that the reputation of Newbury Academy Trust is protected at all times.

IT Users' responsibilities

- Abide by all items in the Computer and Laptop Code of Practice.
- Be responsible for the content of all text, audio or images that are sent using email. All emails should have the employee's name attached.
- Know and abide by all applicable Newbury Academy Trust policies dealing with security and confidentiality of Trust records.
- Inform IT Support if they are aware of any breach in these guidelines.

Monitoring

All messages created, sent or retrieved over the internet are the property of Newbury Academy Trust; use of the internet can be monitored and these records are also property of the Trust. Whilst IT Support does not routinely access or monitor an individual's use of IT systems, there may be instances (i.e. legal, regulatory, security of business reasons) that require mail items/files to be retrieved by IT Support or Capita, our Internet Service Provider (ISP), their authorised agents, or legal/regulatory agencies.

Newbury Academy Trust and Capita reserve the right to retrieve and access any email, whether or not it has been marked confidential, at any time, without the permission of the employee or students and without further notice.

In the instance of email being retrieved to investigate a specific set of circumstances it would be determined why the email inspection was necessary and then two senior members of the Senior Leadership Team would view the content in the first instance.

Any inappropriate use will be reported upon in the appropriate disciplinary procedures, with the involvement of the governors as per the appropriate procedures.

Appendix 1

KS3/4/5 Student Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
6. I will only e-mail or contact people I know, or those approved as part of learning activities
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games and social networks have age restrictions and I should respect this.
13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
14. I am aware that mobile telephones do not run on the school network and shouldn't be used in school unless I have permission from a responsible adult.
15. I am aware that the school rules with internet usage apply while I am in school to any device that can access online material.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 2

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

Appendix 3

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, Virtual learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: [*Newbury Academy Trust Mail]*
- I will only use the approved *email system,* Virtual *Learning Platform (FROG) and trust approved communication systems* with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / E-Safety Coordinator*.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.

- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will follow the school's policy on use of mobile phones.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the *VLE or approved ICT devices* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *Newbury Academy Trust's* child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- *I will only use any Trust/LA system I have access to in accordance with their policies.*
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / *named child protection officer* at the school.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / Safeguarding Lead* on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's e-safety / digital literacy curriculum into my teaching.
- I will adhere and help facilitate the UN convention of Children's rights as set out in the e-safety policy

unicef

Acceptable Use Policy (AUP): Agreement Form
All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.
I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: …… Date: ……..

Full Name: …… (printed)

Job title / Role: ……

Authorised Signature (Head Teacher / Deputy)
I approve this user to be set-up on the school systems relevant to their role

Signature: …… Date: ……..

Full Name: …… (printed)

Appendix 4

E-safety agreement form: parents

Internet and ICT: As the parent or legal guardian of the student(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment (FROG VLE)
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My daughter / son's name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the student is named, we avoid using their photograph.
If their photograph is used, we avoid naming the student.

Where showcasing examples of students work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film.
Only images of students in suitable dress are used.
Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by a child, as part of the learning record, and then sharing with their parent / guardian.
- Your child needing photographic or video evidence as part of their coursework or controlled assessment evidence.
  e.g. a video file of a PE task
- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a video file or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)
In serious cases we will also consider legal options to deal with any such misuse.
The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/
A full copy of the e-safety policy can be accessed through the school website or VLE.

Appendix 5

E-Safety Policy Guidance – What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (Technicians report issue to Sonicwall Helpdesk)
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be. (Technicians report issue to Sonicwall Helpdesk)
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a staff member.

1. Ensure all evidence is stored and logged
2. Inform the Headteacher immediately
3. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
4. Notify governing body.
5. Inform the school technicians and ensure the site is filtered if need be. (Technicians report issue to Sonicwall Helpdesk)
6. Inform the LA if the filtering service is provided via an LA/RBC.
7. In an extreme case where the material is of an illegal nature:
   a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of students accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (undertaken by Headteacher).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police and follow their advice.
   - If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PSHE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, etc.)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including students and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

The school/trust may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent teacher association
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.