Brook Learning Trust
Information Systems Acceptable Use Policy & Statements

At Brook Learning Trust we bring together our unique academies in our belief in the power of education to change lives and communities. It is our steadfast purpose to challenge and defy the barriers that constrain the educational progress of any child. We set high aims for aspiration and secure collective responsibility for all our children's achievements. Our work is underpinned by the values of Integrity, Respect, Courage, Optimism, Excellence and Accountability.

Policy Summary

This policy stipulates the Trust's requirement for responsible use of BLT computer systems and outlines recommended practice to ensure responsible use. It applies primarily to staff and students at the three Trust academies: The Ebbsfleet Academy; The Hayesbrook School and The High Weald Academy; but it applies equally to members of the Trust's administrative teams. This policy should be read in conjunction with the Trust digital communications policy.

The computer information systems and networks referred to (henceforth named the system/s) are owned by the Trust and are supplied for use by students to further their education and by staff to assist them in their professional activities including teaching, research, administration and management.

The Trust reserves the rights of its designated staff to examine or delete any files that may be held on its systems and to monitor any Internet sites visited by users of its systems.

This acceptable use policy has been drawn up to protect all parties: pupils, staff and guests (henceforth referred to as the user(s)) and the Trust.

Use of the systems is conditional upon a user's agreement to practice responsible use (as outlined in this policy).

All users of, and individuals requesting access to, the systems at any premises or operations managed by Brook Learning Trust (BLT) must sign the code of conduct set out below.

System Access

- The systems may not be used for private purposes, unless a member of the Executive Team and/or the Principal has given permission for that use and it does not contravene any rule listed below.
- Staff will only be granted access to the IT systems once their employment start dates are confirmed and their details have been added to the Schools Information Management System (SIMS) by the Trust Human Resources team.
- Students will only be granted access to the IT systems once their starting dates are confirmed and details have been added to the Schools Information Management System (SIMS) by a member of the relevant academy staff.
- Access must only be made via the user's own Trust authorised account and password: details should not be made available to any other person.
- All users will ensure that they log off or lock their screens before leaving any computer unattended (ie when leaving the room). All computers will be shut down at the end of the school day to minimise the risk of unauthorised access (eg by external visitors using facilities out-of-hours). Failure to comply with this instruction will constitute a high risk to the security of the data stored on the Trust's information systems and may result in disciplinary action being taken.

- Activity that threatens the integrity of the system being used, or activity that attacks or corrupts other systems, is forbidden and will result in the user's access being removed.
- The system's security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

Monitoring

- Trust/Academy ICT equipment is monitored for the purpose of safety and security reasons and to safeguard students/staff and trust/academy information systems. All activity is logged or recorded to investigate suspected breaches of this policy. This monitoring extends to live screen capture recording, web browsing, email, instant messaging, as well as documents and file contents.
- Monitoring software is available to staff within ICT classrooms to monitor their own class only
- Monitoring software is used by the ICT Support Team to remotely help users or to administer maintenance on equipment.
- Monitoring will be in accordance with data protection and human rights legislations.

Schools Information Management System (SIMS)

NB This section is for the information of staff only; it is not applicable to students

- Staff users should be aware that information stored in the Trust's systems is private and confidential and should only be shared with the parties whom it concerns as stipulated in the Data Protection Act. See also BLT data protection related policies.
- Users must not distribute or disclose any information obtained from the academy or Trust system to any person(s), with the exception of those to whom the information relates and/or those who have legal responsibility for that person.

Software

- Users must be aware of their legal responsibility to use only licensed software on any system.
- Users must be aware that unauthorised software copies may contain viruses which could affect the integrity of the system; thus unauthorised software must not be used on any workstation.
- Any software downloaded from the Internet, or contained on CD ROMS/USB Storage Devices received through the post or in magazines, should not be loaded without the prior permission of the Network Manager.
- Users are not permitted to copy any software application from an academy or Trust computer system for use outside the academy.
- Unapproved software must not be stored anywhere on the network or attached to email.

Anti-Virus Software

- Anti-Virus protective software is installed on all Trust devices and is updated regularly. This procedure is overseen by the Network Managers.
- Anti-Virus software should not be overridden or turned off at any time. The system automatically virus-checks data files which are added via email attachments and removable storage devices (ie CD ROM, USB drives, etc). The Anti-Virus software is designed to prevent access to infected files and/or to remove any unwanted files or applications that contain a virus.
- If a virus is detected, the user will be notified by an error message and should immediately consult the local Network Manager/ICT support staff member for instruction in dealing with infected files.

Data Transfer

- Any transfer of data from a home computer to the system should only be attempted after virus checking.
- On being made aware that a transferred file is infected with a virus, the user should inform the Network Manager/ICT support staff member for instruction.

- The use of cloud services to store data (eg Dropbox, Box, etc) is forbidden for the reason that these storage services are not guaranteed to be fully compliant with the terms of the Data Protection Act.
- Any data containing personal details must not be taken off-site, stored on personal removable media or sent to personal email addresses, etc.
- Data stored on the system in common areas are the property of the Trust and should not be copied and/or removed from the site.

Internet Access

- All Internet activity should be appropriate to the user's professional activity or education; appropriacy is described in this policy and will be further outlined, in response to users' queries, by Network and Line Managers and/or Principals.
- Internet use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The copyright of materials must be respected: I will reference all information I include in my work which I have sourced online and will not use material protected by copyright restrictions.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Use of chat rooms, dating and social media websites is not allowed.
- Use of gaming websites is not allowed.
- Use of websites or applications to circumvent the Trust's web filtering, in order to access blocked websites, is forbidden.
- Use of the system to access inappropriate materials such as pornographic, racist or other such offensive material is forbidden.
- Access to personal email accounts may be blocked.

Email

- Users are responsible for all email sent and for contacts established which may result in email being received.
- Email should be worded in a manner appropriate for a professional educational institution, particularly as messages may be forwarded, inadvertently sent to the wrong person, printed and otherwise seen by unintended recipients.
- Students who receive offensive email must immediately tell a teacher.
- Staff who receive offensive email must immediately tell a member of SLT or the Trust Executive.
- Email should be used for Trust and academy purposes only.
- Personal use of the email system is forbidden. Trust and academy email addresses may not be used for signing up to social networking/media sites, shopping sites, personal banking or other sites unrelated to the Trust.
- Personal emailing or messaging between staff and students is not permitted.
- Email should not be sent or forwarded to personal accounts outside the Trust's systems.
- Email communications between staff and students: messages must be restricted to Trust/academy email addresses.
- Students must not reveal personal details of themselves or others in email communications and must never use the system to arrange to meet anyone unknown to their families.
- Emails sent to parents and to external agencies in furtherance of Trust activities may only be sent using a Trust/academy email account; messages should be worded appropriately, using the same stylistic conventions as a letter written on Trust or academy headed paper.
- The forwarding of chain letters/emails via Trust/academy email addresses is not permitted.
- Staff/Student photographs are displayed in the Outlook Address Books of all Trust/academy users, to assist identification. These photographs are only visible by users inside the Trust/academy email systems.
- Trust/academy email accounts may be accessed on personal devices such as laptops and smartphones on the basis that these devices will be required to have a passcode/password.
- In the event that a device to which Trust/academy data have been downloaded is lost or compromised, the Network Manager reserves the right to erase the device remotely.

- Sensitive information regarding student welfare should be sent using the SIMS.net message facility and NOT via the Trust/academy email system, in order to preserve confidentiality and ensure the protection of students' personal data.
- Users should be aware that email communications are monitored; the Trust reserves the right to access Trust/academy email accounts at any time.

External Hosted Services

- The Trust/Academies may use external companies to provide extra services to staff/student/parents; these could include:
  - Learning materials
  - Homework Systems
  - Virtual Learning Environment (VLE)
  - Parents Evening Systems
  - Reporting Systems
  - Communications systems
  - Payment Systems

  Account and password details associated with these systems should not be made available to any other person.

Remote Access

- Remote access is provided to allow users access to Trust/academy software.
- Remote access is provided in order that users can access data stored on the system and thus to avoid the transfer of data to personal devices off site.
- Remote access is provided to facilitate access to management and other sensitive data which must remain on the system and not be transferred to personal devices.
- Remote access via public computers and from public locations, ie libraries, cafés, etc, is discouraged given the confidential nature of the information available through SIMS and other systems.
- Copying software and/or data from the remote server is not permitted.

Printing

- Printing in Trust premises is to be used for business purposes only.
- Printers are automatically set to double-sided (duplex) to save paper.
- Colour printing should only be used for final copies of documents.
- Users are supplied with departmental printing codes. Departments are allocated monthly printing budgets, the value of which are determined by the Trust Finance Director. Print budget balances are reset on the first day of each calendar month. It is the responsibility of all department members to ensure that they monitor their budget use in line with their printing requirements for the entire duration of each month.
- Users will undertake not to print documents stored electronically and/or emails unless a hard copy is specifically required
- Requests for additional printing budget allowances must be made to the relevant Network Manager via the ICT Helpdesk. This will only be authorised under certain conditions.

Bring Your Own Device (BYOD)

- Users are responsible for their own device/s and use them at their own risk. The Trust is not responsible for any damage, loss or theft of personal devices used on site.
- Users wishing to use their own device should ensure it has appropriate and up to date anti-virus software installed.
- Internet access on personal devices is filtered in the same manner as access on the Trust's devices; users will be required to login using their Trust network credentials in order to access the Internet.

- Personal devices can, however, be configured by the Network Manager/ICT support staff for Wi-Fi access to the Internet from Trust sites. The Trust accepts no liability when configuring a personal device for use on its networks; repair or upgrade of a device is the owner's responsibility and will not be undertaken by Trust personnel.

Personal Mobile Phones and Tablets

- Use of personal mobile phones and tablets is governed by the relevant academy policy which will stipulate site areas and times of the school day during which use is permitted, if any.

- Staff are not permitted to use their personal mobile phones or tablets for contacting students or their families in their professional capacity.

- Staff and visitors are not permitted to use personal mobile phones or devices to take photos or video footage of students: only devices owned by the Trust should be used for these purposes for professional purposes by Trust employees only.

Storage of Data

- Users are provided with an area on the system in which to save their work; these data will be backed up on a regular basis. Storage of personal items on the system is not permitted.
- Storing digital copies of films on the system is not permitted unless they have been uploaded by the Network Manager/ICT support staff to the system in accordance with the licences with which they were purchased.
- Storing digital music collections on the system is not permitted unless they have been uploaded by the Network Manager/ICT support staff to the system in accordance with the licences with which they were purchased.
- Storing documents: some documents are governed by user agreements that do not permit their storage on a network; these documents must remain on the original media on which they were sent.
- Files held on the system are regularly checked for compliance with this policy.

Trust Equipment

- All equipment owned by the Trust is security marked and any mobile devices are assigned to a user who is responsible for that device.
- Users are responsible for the equipment that they use. A record of user access to the device is kept and any damage to the equipment will result in a cost incurred by the user for repair or replacement where necessary.
- Any equipment that is loaned to a user must be returned either when leaving the Trust's employment or on request by a Line Manager or by the Network Manager. Failure to return equipment will result in a cost incurred by the user.
- Academy staff are responsible for Trust equipment used in classrooms and will check that all devices are working correctly and without damage at the start and end of each lesson.
- Any damage to equipment must be reported immediately to the Network Manager/ICT support staff via the IT Helpdesk portal.

Identification (ID) Badges

- ID badges must be worn on site at all times. Certain users' badges can be used to open specific gates/doors/rooms or used with other systems ie signing-in to a site, for restaurant purchases and use of printers, photocopiers, etc.
- In the event that your ID Badge is lost you should immediately notify the issuing party to ensure that the badge is deactivated and replaced.
- Badges must not be shredded / leant to another person / passed to anyone else, whether an employee of the Trust or not.
- Badges must be returned to a member of the Human Resources Team or the Network Manager at the end of a member of staff's employment.

Protecting the Environment: avoiding unnecessary use of Power and Resources

- Users are asked to turn off when not in use, and at the end of each day, the following equipment:
  - Computers
  - Projectors
  - Printers
  - Speaker Systems
  - DVD players
  - Visualisers and any other relevant device
- Trustees, academy councillors and all meeting attendees will be encouraged to refer to previously emailed documents via an electronic device brought to the meeting in preference to requesting Trust staff to print paperwork packs.

ICT Support

- All ICT support requests must be submitted via the ICT Helpdesk.

Irresponsible Use

- Users are liable for any misuse of the system and/or breach of the Data Protection Act that may occur as a result of their failure to adhere to any of the rules/guidelines listed in this document.
- The Trust reserves the right to revoke or deny access to the system where a user or users is/are found to be in breach of this policy.

Procedure

Each user will be asked to sign the Information Systems Acceptable Usage Statement (see next page) before being cleared for access to the system. Statements signed by each employee, student and guest will be kept on file at the academies or in the Trust offices as appropriate

POLICY REVIEW AND RATIFICATION

Policy reviewed bi-annually and ratified by BLT Audit & Risk Committee in December

This review by Network Managers in consultation with Safeguarding Leads (DSLs)	June 2017
Summary of amendments to this iteration:	Addition of a section on mobile phones and devices; expansion of the section on emails; considerable re-wording of all sections to ensure that all related matters are covered comprehensively in this policy and the BLT digital communications policy. The two documents should be read in conjunction.
Ratified by BLT Audit & Risk Committee	June 2017
Next review	December 2018 to comply with new policies review schedue

Brook Learning Trust

Information Systems: Acceptable Use Policy

Staff / Visitor Statement

signed in confirmation of policy compliance
prior to system access being granted

Please read through this policy and initial each page at the bottom in the space provided.
Please complete the following in BLOCK CAPITALS, sign
and return to the Network Manager or issuing member of staff

Full Name: .....

Staff / Visitor: .....

Trust / Academy: .....

Position in
Trust / Academy: .....

.....

Signature: ..... Date: .....

Access granted by: ..... Date: .....

Initials _____

Brook Learning Trust

Information Systems: Acceptable Use Policy

Parent/Carer Statement

To be signed before student access to the system is granted

- I have read and discussed the relevant sections of the Trust Acceptable Use Policy (attached) with my child.
- I know that my child will receive online safety (e-safety) education in understanding the importance of safe use of technology and the Internet, both in and out of school.
- I am aware that all use of academy equipment may be monitored for safety and security reasons and to safeguard both my child and the Trust information systems. This monitoring will be in accordance with data protection and human rights legislation.
- I understand that the academy will take all reasonable precautions to ensure that students cannot access inappropriate materials from school.
- I understand that the Trust cannot be held responsible for the content of materials accessed through the Internet and is not liable for any damages arising from use of the Internet facilities.
- I understand that, if academy staff have any concerns about my child's safety online, either at school or at home, then I will be contacted to discuss this.
- I understand that, if my child does not abide by the Information Systems: Acceptable Use Policy, then sanctions will be applied in line with relevant academy and Trust policies. If there is reason to suspect that my child has committed a criminal offence, the Police will be contacted.
- I will support the Trust's approach to online safety (e-safety) and discuss online safety with my child/ren at home.
- I know that I can approach academy staff (particularly the Designated Safeguarding Lead) Coordinator and/or a member of the Senior Leadership Team if I have any concerns about online safety (e-Safety).
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online.

I confirm that I have read the BLT Information Systems: Acceptable Use Policy and agreed with the statements above

Child's Name…… Year & Class …….

Parent's Name……..

Parent's Signature……. Date……..

Initials _____

Brook Learning Trust

Information Systems: Acceptable Use Policy

Student Statement

To be read and signed before using the system

- I know that computers and Internet access have been provided at the academy to support my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I know that my use of academy computers and my Internet access will be monitored; this will be conducted in accordance with data protection and human rights legislation.
- I will keep my password safe and private to protect my privacy.
- I will protect my personal information online at all times.
- I will write emails and online messages carefully and politely as I know they could be forwarded to someone else.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting, I will immediately talk to an adult.
- I recognise that bullying in any form (on and off line) is not acceptable and I know that technology should not be used for harassment.
- I understand that it is not allowed by the academy, and may be a criminal offence, to download or share inappropriate pictures, videos or other material sourced online.
- I understand that it is against the law to take, save or send indecent images of anyone under the age of 18 as explained at www.thinkuknow.co.uk
- I will not attempt to access or change other people's electronic files, accounts or information.
- I will not download images or videos to the information system without permission of a teacher.
- I will only use my mobile phone/tablet or other device in school if I have permission to do so and if using it is in accordance with academy policy.
- I will reference all information I include in my work which I have sourced online and will not use material protected by copyright restrictions.
- I will always check that any information I source online is reliable and accurate.
- I will only change the settings on an academy computer I am using when permitted by a teacher/technician.
- I know that use of the information system for personal financial gain, gambling, political purposes or advertising is not allowed.
- I understand that the academy's Internet filter is there to protect me, and I will not try to bypass it.
- I know that, if academy staff suspect that I am using the Internet inappropriately, then checks will be made which may result in the confiscation of my mobile phone/tablet or other device.
- If I am aware of anyone at the academy using the Internet inappropriately, I will report this to a member of staff.
- I will speak to an adult I trust if something happens, online or off line, to me or another student which makes me feel worried, scared or uncomfortable.
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

I confirm that the BLT Information Systems: Acceptable Use Policy has been explained to me. I agree with the statements above

Name of Student …….

Year & Class ……....

Student's Signature……. Date……..

Initials _____