| | |
|---|---|
| **Title** | Acceptable Use Policy |
| **Associated Policies** | • Safeguarding and Child Protection (TPO/HS/05)<br>• Professional and Safe Conduct (TPO/STA/10)<br>• Data Protection (TPO/STA/25)<br>• Freedom of Information (TPO/QA/03)<br>• Online Safety (TPO/STA/12) |

REVIEWED: April 2020 NEXT REVIEW: September 2020

## 1. Policy Statement

**1.1** Brooke Weston Trust acknowledges that IT is an integral and critical resource for students, staff, governors, volunteers and visitors through the delivery and support of teaching and learning and supporting pastoral and administrative functions of the Trust and its academies. However, the IT resources and facilities our academies use also pose risks to data protection, online safety and safeguarding.

**1.2** The aim of this policy is to:

- Set guidelines and rules on the use of school IT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the Trust and academy communities engage with each other online
- Support the Trust's policies on data protection, online safety and safeguarding
- Prevent disruption to the Trust and academies through the misuse, or attempted misuse, of IT systems
- Support the school in teaching students safe and effective internet and IT use

**1.3** Brooke Weston Trust provides information systems for the use of all staff, students, governors and volunteers on the understanding that:

- The user has read and agreed to abide by this policy.
- The user does not misrepresent him/herself or attempt to impersonate any other person or entity whilst using Trust IT systems.
- The user does not publish libellous material using the Trust IT systems e.g. Via blogs or online journals or videos published on social media.
- Brooke Weston Trust reserves the right to suspend access, retain equipment loaned to staff or students and view any data held on its systems whilst investigating a breach of this policy or whilst investigating any other matter in which Brooke Weston Trust has a legitimate interest.

**1.4** The Trust and its individual academies have the right to monitor the use of all devices including mobile devices issued, for internet use, e-mails and all aspects of the network/computer system. Further detail is included within paragraph 5.9 of this policy.

**1.5** Any student, staff member, governor or volunteer who are in breach of this policy and engage in any of the unacceptable activity covered under the policy may face disciplinary action in line with the Trust's respective disciplinary policies. Depending on the nature of the breach, other sanctions such as revoking permission to use the Trust's IT systems, may be considered where appropriate.

**1.6** This policy has been developed to comply with: Data Protection Act 2018, The General Data Protection Regulation, Computer Misuse Act 1990, Human Rights Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Education Act 2011, Freedom of Information Act 2000, The Education and Inspections Act 2006, Keeping Children Safe in Education 2019, and Searching, screening and confiscation: advice for schools.

## 2. Who does this policy apply to?

**2.1** This policy applies to all 'users' of Brooke Weston Trust information and relates to use of all IT facilities provided by the Brooke Weston Trust (see paragraph 4 for definitions).

**2.2** This policy applies not only to use of Trust digital technology equipment in school but also applies to the use of Trust systems and equipment off school premises and the use of any personal devices or equipment on or off school premises.

## 3. Who is responsible for carrying out this policy?

**3.1** The implementation of this policy will be monitored by the Senior Leadership Team and the governors of the Academy and will remain under constant review by Brooke Weston Trust.

## 4. Definitions

**4.1** **IT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the IT service.

**4.2** **Users:** anyone authorised by the school to use the IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

**4.3** **Personal use:** any use or activity not directly related to the users' employment, study or purpose.

**4.4** **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities.

**4.5** **Materials:** files and data created using the IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

## 5. Procedures

**Access**

**5.1** Access to the Trust's information systems and user accounts is obtained via a unique username and password. This is provided to the user by the IT Support team on the understanding that:

- Any password issued to a user becomes his/her responsibility. No password should be shared with other users or third parties.
- Sharing a password may result in suspension of the user's account.
- Using the account of another user will result in immediate suspension of access to the Academy's systems and referral to the Senior Management Team for consideration under the Trust's disciplinary procedures.
- The only software authorised for use on Brooke Weston Trust information systems are those programs already installed on the machinery by the IT Support team or authorised for use in Trust activities. This includes online/Cloud services. Any attempt to introduce or install software onto the Academy systems will be viewed as an intention to damage Brooke Weston Trust property and could constitute a breach of safeguarding and/or data protection regulations, resulting in disciplinary action.
- Any user who causes damage, directly or indirectly, to any equipment may be refused the right to further use of the equipment and billed for its repair or replacement.
- Gaining, or any attempts to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel will be considered unacceptable use and a breach of this policy

**5.2** Other examples of unacceptable use following access to an academy's information system include (but is not limited to):

- Using the Trust's IT facilities to breach intellectual property rights or copyright

- Using the Trust's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Activity which defames or disparages the school or Trust, or risks bringing the school or Trust into disrepute. This includes canvassing, lobbying, advocacy, or personal endorsement that has not been ratified by the Trust.
- Sharing confidential information about the school, its pupils, or other members of the school community
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Promoting a private business, unless that business is directly related to the school

**Storage**

**5.3** All users are provided with storage space for their files on the Trust's servers referred to as the user's Home Area. This storage is provided on the understanding that:

- All data is stored in the approved area (my Home Directory/OneDrive area). Any data saved in areas other than approved locations may not be backed up by the IT team
- No inappropriate material is stored e.g. pornography or libellous material.
- No material is stored that infringes copyright i.e. illegal copies of any audio or video file or software program.
- No personal information about others is stored without direct reference to the Data Protection Act.
- Brooke Weston Trust reserves the right to withdraw access to files and materials whose ownership is in question whilst an investigation is carried out.
- Users may not use the Trust's IT facilities to store personal non-work-related information or materials (such as music, videos, or photos). Use of the Trust's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities (see paragraph 1.4). Where breaches of this policy are found, disciplinary action may be taken.

**Internet**

**5.4** Brooke Weston Trust provides access to the Internet in as unrestricted a manner as possible on the understanding that:

- No user will access, download, store, bookmark or record websites containing inappropriate content.
- No user will access websites containing online games or instant messaging services.
- No user will attempt to access online shops or services whose age requirements they do not meet e.g. eBay or any other websites which are not relevant for work purposes.
- Brooke Weston Trust reserves the right to filter or restrict access to certain Internet sites. Any attempts to bypass the Trust's filtering mechanisms will be considered unacceptable use of the Trust's IT systems.
- Staff will adhere to the Trust's Professional and Safe Conduct policy with particular regard to use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

**Mail**

**5.5** Electronic mail accounts are provided for everyone at Brooke Weston Trust on the understanding that:

- The content of any mail sent will be appropriate in terms of its language and subject matter regardless of its destination. Users will take care with the content of all email messages, as

incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract

- The email account will be used for work/study purposes only. All work/study-related business should be conducted using the email address the school has provided. Staff must not use personal email accounts when communicating with parents and students.
- Users will comply with the provisions as set out in the Trust's Data Protection Policy particularly in relation to the following:
    - when sending sensitive or confidential information by email. For example, any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Any data breaches will be reported in line with the Data Protection Policy
    - raising any concerns to the IT Support team regarding any suspicious hyperlinks in emails or any attachments to emails, unless the source is known and trusted
- No harmful software will be intentionally transmitted with any message.
- No chain-email messages will be originated by the user or forwarded on from his/her account.
- Brooke Weston Trust reserves the right to suspend access to the mail system for any user.
- Brooke Weston Trust reserves the right to intercept and monitor any message traffic if it suspects inappropriate content, use of offensive language or malpractice.
- Access to email will terminate when a user leaves the Academy/Trust.

**Social Media**

**5.6** Each academy has an official social media page, managed by specific appointed members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

**5.7** Those who are authorised to manage or post to the account must abide by the guidelines as prescribed by their individual academy.

**Data security**

**5.8** The Trust takes steps to protect the security of its computing resources, data and user accounts. Further detail of these measures are included within the Trust Data Protection Policy. All staff are required to be familiar with and comply with the contents of this policy.

**Monitoring of academy networks and use of IT facilities**

**5.9** The Trust and its individual academies have the right to monitor the use of all devices including mobile devices issued, for internet use, e-mails and all aspects of the network/computer system for purposes such as:

- Ensuring effective academy and IT operations including:
    - resolving a technical issue;
    - checking for viruses or other network threats
    - updating and maintaining devices/software belonging to the school
    - checking compliance of devices/software belonging to the school
    - obtaining information related to academy business
- investigating unauthorised use where there is a breach with academy policies, procedures or standards;
- prevention or detection of crime
- compliance with a Subject Access Request, Freedom of Information Request or any other legal obligation

**5.10** Any staff with concerns about any illegal, inappropriate or harmful material or incident that they become aware of must immediately be reported to their line manager or appropriate person.

**Mobile devices provided by the Brooke Weston Trust**

**5.11** Any mobile device provided to a member of staff or student by the Trust is used subject to the following terms as set out in this policy.

**5.12** In the case of staff laptops the machines are configured so that these terms are displayed as a reminder whenever it is switched on:
*This is a Brooke Weston Trust computer system, which may be accessed and used by authorised personnel and subject to compliance with Brooke Weston Trust policies, in particular the Acceptable Use Policy. Unauthorised access or use of this computer system may result in criminal, civil, regulatory and/or administrative action. All information on this computer system may be monitored, recorded, read, copied and disclosed by and to authorised personnel for official purposes, including criminal and regulatory investigations. There is no right to privacy on this system except where required by law. Access or use of this computer system by any person, whether authorised or unauthorised, is subject to these terms.*

**5.13** Where provided, staff must use Trust-issued mobile phones when contacting parents or students. Under no circumstances should staff be providing their personal phone numbers to parents or students. Staff must use phones provided by the school to conduct all work-related business.

**5.14** Any damage or faults involving mobile devices provided by the Trust must be immediately reported to the IT support team.

## 6. Policy Review

**6.1** This policy will be monitored as part of the Trust and Academy's annual internal review and reviewed on a three-year cycle or as required by legislature changes.

| | |
|---|---|
| **Title** | Annex to the Acceptable Use Policy for Online Learning: COVID-19 |
| **Associated Policy** | • Acceptable Use Policy (GU/06)<br>• Safeguarding and Child Protection (TPO/HS/05)<br>• Professional and Safe Conduct (TPO/STA/10)<br>• Data Protection (TPO/STA/25)<br>• Freedom of Information (TPO/QA/03)<br>• Online Safety (TPO/STA/12) |

REVIEWED: April 2020 NEXT REVIEW: September 2020

## 1. Policy Statement

**1.1** This Annex to the Brooke Weston Trust Acceptable Use Policy has been created in response to the COVID-19 pandemic. From 20th March 2020 parents and carers were asked to keep their children at home, wherever possible, and for schools to remain open only for selected students who absolutely need to attend. Schools and all childcare providers were asked to provide care for a limited number of children namely children who are vulnerable, and children whose parents are critical to the COVID-19 response and cannot be safely cared for at home.

**1.2** This Annex must be read in conjunction with the Brooke Weston Trust Acceptable Use Policy. Guidance from the DFE is being reviewed and updated regularly as we navigate through these unprecedented times and therefore this Annex will also be updated as required.

**1.3** This Annex of the Brooke Weston Trust's Acceptable Use Policy contains details of our reviewed safeguarding arrangements in the following areas:

- Online Learning (Microsoft Teams)
- Reporting Online Safeguarding Concerns
- E-safety
- Code of Conduct – ICT Acceptable Use

## 2. Who does this annex apply to?

**2.1** This Annex applies to all volunteers, students, visitors, governors, parents or carers and staff working for The Brooke Weston Trust.

## 3. Who is responsible for carrying out this annex?

**3.1** The Principal is responsible for implementing this policy.

## 4. What are the principles behind this policy?

**4.1** Brooke Weston Trust is committed to ensuring that during school closure, teachers will provide learning activities for students to complete at home. This may include use of online learning platforms.

## 5. Procedures

**Online Learning (Microsoft Teams)**

**5.1** Brooke Weston Trust utilises Microsoft Teams as the learning platform and provides unrestricted communication to staff classes and student groups on the understanding that:

- All users will only use Microsoft Teams to teach students and communicate with colleagues in a school capacity.
- When communicating on Microsoft Teams, it is important that:
  - Staff are appropriately dressed and in a setting which allows them to have a professional meeting
  - Staff and students do not inappropriately use the chat function (this can be blocked within classes and by admin)
  - Staff and students should not use the video functionality when teaching. It is recommended that students switch off their microphones to limit issues and can use the chat functionality to ask questions. If it is deemed appropriate a student can activate their microphone but should be appropriate. Lessons delivered must be recorded to protect staff and students.
  - Staff should record, the length, time, date and attendance of any online teaching sessions held
  - There should be no 1-1 teaching. If it if absolutely necessary, prior agreement must be sought from the Principal and must be recorded - even voice only
  - Safeguarding staff may conduct 1-1 meetings and these must be recorded unless it compromises the student disclosing. A risk assessment must be completed in this situation
  - Language must be professional and appropriate, including any family members in the background
  - Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
  - You are mindful of confidentiality as you will be working from home. Ensure that no one else can see your screens when sending information and always lock your laptop when you are not working, even if it is only for a minute or two. Do not discuss students with anyone other than work colleagues and take care that you cannot be overheard.
  - Staff should record, the length, time, date and attendance of any sessions held.

**5.2** Although online assessment packages such as Hegarty maths, Seneca, SAM Learning, GCSE Pod, etc. can be used it is important that the software is suitably age restricted and that communication within those packages are kept to a minimum. Software used should be agreed to by the IT team and your line manager within school.

**5.3** External software must have relevant security measures in place and should for example meet industry standards. Personal information should be limited with these packages, for example student login details could be their Admission number within school so that names and surnames, etc. are not shared. For example 12345@brookewestontrust.org.

**5.4** No user will access, download, store, bookmark or record websites containing inappropriate content. It is also important that users do not direct students to websites that contain inappropriate content or have unsuitable age restrictions. Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parental permission. All video links should be checked for age-appropriateness before distributing to students.

**5.5** **No other learning platforms, social media or video conferencing can be used for online remote teaching**.

**Reporting Online Safeguarding Concerns**

**5.6** We have a responsibility when it comes to e-safety and need to ensure the school's online procedures keep children and young people safe.

**5.7** If you think a child is in immediate danger, contact the police on 999. If you're worried about a child but they are not in immediate danger, you should share your concerns with the schools Designated Safeguarding Lead and follow your school's child protection procedures (e.g. CPOMS).

**5.8** Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

**5.9** It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

**5.10** Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline. Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation

**5.11** Reporting online child abuse images

It's against the law to produce or share images of child abuse, even if the image was self-created. This includes sharing images and videos over social media. If you see a video or image that shows a child being abused:

- Don't comment, like or share the video or image, as this will distribute it further
- Report it to the website you've seen it on

**Report it to your Designated Safeguarding Lead**

**E-safety**

**5.12** Principals will ensure that relevant e-safety advice for students and parents/carers is available through the schools website/other appropriate means.

**5.13** Information and support for children and young people about staying safe online can be found at:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

**5.14** Information and support for parents and carers to keep their children safe online includes:

- National Online Safety – produces a wide range of parent guides
- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and careers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers

## 6. IT Acceptable Use Code of Conduct for Staff:

**5.15** I understand that I must use the Trust's IT facilities in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, other users and students. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

**5.16** In addition to adhering to the Acceptable Use Policy detailed above and the Trust's Professional and Safe Conduct Policy, I will comply with the below code of conduct which has been developed to ensure my professional and personal safety when delivering online learning.

**5.17** **For my professional and personal safety:**

- I understand and accept that the Trust will fully monitor my use of the school digital technology and communications systems.
- I understand that if my activity causes any concerns, safeguarding software installed across the Trust may automatically alert appropriate safeguarding specialists who may choose to investigate depending on the content of the alert.
- I understand that the rules set out in this agreement also apply to use of Trust provided ICT technologies (e.g. laptops, email, data etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will always lock or sign out of any device I am not actively using or will be leaving unattended.
- I will only use chat and email functionality on Trust issued devices.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, my line manager or appropriate person.
- I will immediately report and potential data breaches to the Headteacher/GDPR Nominated contact.
- I will only use equipment that is provided by the Trust for teaching and school-related activities.
- I understand that if I leave the Trust, all my digital accounts will be suspended and my data deleted at the Trust's discretion.

**5.18** **I will be professional in my communications and actions when using Trust systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Trusts GDPR policy guidance on consent for digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so.
- If I am responsible for updating social networking sites on behalf of the school, I will do so in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities. This includes canvassing, lobbying, advocacy, or personal endorsement that has not been ratified by the Trust.

**5.19 Ensuring safe and secure access to technologies and ensure the smooth running of the online platform (Teams):**

- When I use my personal digital device (e.g. personal laptop/tablets/phones) at home, I will follow the rules set out in this agreement and need to ensure that I am using the device on a secure network.
- I will not use personal email addresses for academy/Trust ICT services nor to register for any services on behalf of the school.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) I will contact the ICT Support team for advice
- I will ensure that I place my data in my approved areas (my Home Directory/OneDrive area) or a shared area if appropriate and I have been given access. If I house data anywhere else other than these approved locations I understand that the school IT service will not back it up and I will take responsibility for backing up any such data. I will not house any personal data on any Trust system.
- I will not try to upload, download or access any materials which are illegal (any data covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have been given permission to.
- I will not disable or cause any damage to school/academy equipment, or any equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection GDPR Policy. Where digital personal data is transferred outside the secure local network, you must take the necessary steps to ensure that the data is shared securely by either encrypting, password protecting or the use of Office365. Paper based protected and restricted data must be held in lockable storage.
- I understand that GDPR law requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not share my personal email address or phone number with students or parents.

**5.20 When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**5.21 I understand that I am responsible for my actions inside and outside of the Trust:**

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology equipment in school, but also applies to my use of Trust systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Trust
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action in line with the Trust's Disciplinary Policy.

**5.22** I have read and understand the above and agree to use the school digital technology systems for Online Learning and my own devices within these guidelines.

Signed: Date:

**Information Systems Acceptable Use Policy for Students**

**5.23** All students will have signed this document when they joined the school. Principals should ensure that children and young people are aware of their responsibilities when using Microsoft Teams.

## 6. Policy Review

**6.1** As required by government updates or September 2020, whichever is sooner.