Title	Acceptable Use Policy
Associated Policies	• Safeguarding and Child Protection (TPO/HS/05) • Professional and Safe Conduct (TPO/STA/10) • Data Protection (TPO/STA/25) • Freedom of Information (TPO/QA/03) • Online Safety (TPO/STA/12) • Electronic Communications – Use and Management

REVIEWED: September 2024 **NEXT REVIEW: September 2026**

1. Policy Statement

1.1 Brooke Weston Trust (the Trust) acknowledges that Information Technology (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.
- Promote safe working practices for staff and students for remote learning

1.3 The 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 5.10 of this policy.

1.5 Any student, staff member, governor, volunteer or visitor 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, 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 and services 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.

2.3 All users will sign the relevant Acceptable Use Policy documents (Appendices A-D) as required.

3. Who is responsible for carrying out this policy?

3.1 The implementation of this policy will be monitored by the Senior Leadership Team, the governors within each academy and Trust Central Team 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:** staff 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. This includes files and data created by users through use of Artificial Intelligence (AI).

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/their 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/Trust's systems and referral to the Senior Leadership 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 services. Any attempt to introduce or install software onto the Academy or Trust 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 and services to breach intellectual property rights or copyright.
- Using the Trust's IT facilities and services 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 area and/or Office 365 storage via OneDrive or SharePoint). Any data saved in areas other than approved locations may not be backed up by the IT team.
- Data is stored in line with the Trust's retention schedule (see Data Protection policy)
- 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 or services to store personal non-work-related information or materials (such as music, videos, or photos). Use of the Trust's IT facilities or services 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 unless it has been an identified learning function which has been agreed by the Principal.
- 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 and other forms of electronic communication

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

- Staff will only communicate with students by email using their, and the students', school email address. Staff should not contact students outside of official working hours or Academy sanctioned extra-curricular activities, unless in exceptional circumstances. Staff should never contact students via a private/personal phone and/or email account.
- 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.
- Staff will report to the Principal, immediately, any communication received from students or parents/carers where there appears to be a blurring of boundaries with regards to the relationships between students, staff and families.
- 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 The Trust and each academy has an official social media page(s), 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 and by the guidelines of the site. Please refer to the Professional and Safe Conduct Policy regarding expectations of staff and use of social media.

5.8 All staff must be mindful about interacting with official academy or Trust social media accounts (e.g., liking or sharing content) when using their own social media profiles, as this will highlight personal accounts to wider members of the academy community.

Data security

5.9 The Trust takes steps to protect the security of its computing resources, data and user accounts. Further detail of these measures is 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 and services

5.10 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; and
- compliance with a Subject Access Request, Freedom of Information Request or any other legal obligation.

5.11 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

5.12 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.

5.13 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.

5.14 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.

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

6. Remote Learning Platform - Microsoft Teams

6.1 In some rare cases, learning will be delivered online by academies depending on circumstances of the academy or individual students.

6.2 The temporary provisions in the Coronavirus Act 2020 expired on 24 March 2022. However, academies will follow the DfE's non-statutory guidance on Providing Remote Education (2024) in cases where it is not possible or contrary to government guidance for some or all pupils to attend face-to-face education. The Education Endowment Foundation (EEF) has found that the effectiveness of remote teaching is determined by many of the same factors as determine the effectiveness of live classroom teaching. For example:

- ensuring pupils receive clear explanations

- supporting growth in confidence with new material through scaffolded practice
- application of new knowledge or skills
- enabling pupils to receive feedback on how to progress

Where online learning is required, the Trust believes that reasonable endeavours should be made to ensure that remote learning is as effective as possible, ensuring that students are safe online.

6.3 Principals will signpost the relevant online safety advice for students and parents/carers available through the schools' website/other appropriate means.

6.4 Principals will ensure that students receive appropriate information and guidance about how to access and behave during remote learning sessions.

6.5 Brooke Weston Trust approves and utilises only Microsoft Teams as the learning platform for online learning directly provided by Trust academies, 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.
- Communication via Teams would normally be in the school setting, where this is not possible, communication from home is allowed. In either event it is essential that:
    - Staff are appropriately dressed and in a setting which allows them to have a professional meeting, including confidential if relevant
    - Staff and students do not inappropriately use the chat function (this can be blocked within classes and by admin)
    - Only staff may use the video/broadcasting functionality
    - 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 and stored according to guidance by the Principal.
    - Staff should also record, the length, time, date and attendance of any online teaching sessions held (Appendix E)
    - 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 and pastoral staff may conduct 1-1 meetings and these must be recorded unless it compromises the student disclosing. A risk assessment (Appendix F) must be completed in this situation, which must be signed by the Principal (or other delegated person).
    - Meeting facilitators must ensure that language is professional and appropriate at all times
    - Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
    - You are mindful of confidentiality if working from home. Ensure that no one else can see the screens when sending information and always lock your laptop when 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. See Appendix E for suggested format.
- 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. All software used must be agreed to by the Principal (or person with delegated responsibility) and your line manager within school.

- 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.
- 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.

6.6 Reporting Online Safeguarding Concerns
We have a responsibility when it comes to online safety and need to ensure the school's online procedures keep children and young people safe.

6.7 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).

6.8 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).

6.9 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
- using Artificial Intelligence
- voice chat in games.

6.10 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)
- being pressured or coerced in to creating and sharing sexual imagery
- sexual abuse and online sexual harassment
- sexual exploitation

6.11 Reporting online child abuse images
Whilst the law is designated to safeguard rather than criminalise children and young people, it is against the law to create, possess or share sexual images or videos of a child, even if the image was self-generated. 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 the Internet Watch Foundation or National Centre for Missing and Exploited Children
- **Report it to your Designated Safeguarding Lead in line with the Safeguarding and Child Protection Policy (but without sharing the images or videos directly).**

6.12 Further information can be found in the Online Safety Policy and Safeguarding and Child Protection Policy.

7. Policy Review

7.1 This policy will be monitored as part of the Trust and Academy's annual internal review and reviewed on an annual basis or as required by legislature changes.

Document Control

Date of last review:	September 2024	**Author:**	Trust Safeguarding Officer
Date of next review:	September 2026	**Version:**	6
Approved by:	Safeguarding Review Group	**Status:**	Ratified

Summary of Changes: V5

- Removed reference to the Covid-19 pandemic ***(paragraph 1.2)***
- Updated Keeping Children Safe in Education and Searching, Screening and Confiscation guidance ***(paragraph 1.6)***
- Inserted that staff should not contact students outside of official worker hours or Academy sanctioned extra-curricular activities, and should never contact students via private or personal accounts ***(paragraph 5.5)***
- Inserted that staff will report to the Principal any communication received from students and parents which appears to indicate a blurring of professional boundaries ***(paragraph 5.5)***
- Updated guidance relating to the provision of report education ***(paragraph 6.2)***
- Inserted reference to online sexual harassment ***(paragraph 6.10)***
- Updated to Staff Acceptable Use Policy to strengthen content relating to:
    - Password security; reporting harmful content; online reputation; taking and storing images of students on personal devices, and promoting online safety with students
- Updated the KS3 – 5 Acceptable Use Policy to strengthen content relating to:
    - Online reputation; relaced the term 'indecent images' with 'any naked image or video of anyone under 18, for clarity; critical evaluation of online content

Summary of Changes: V6

- Updated references to Keeping Children Safe in Education throughout
- Included Artificial Intelligence within the scope of the policy ***(Paragraphs 4.5 and 6.9)***
- Added that staff must be mindful that using their personal social media accounts to engage with academy or Trust social media content will highlight their private accounts to the wider academy community ***(paragraph 5.8)***
- Clarified that the law relating to indecent images of children is designed to safeguard rather than criminalise young people and included links to the Internet Watch Foundation and the National Centre for Missing and Exploited Children ***(paragraph 6.11)***
- Updated the Staff Acceptable Use Policy to include reference to Artificial Intelligence and expanded the reference to not taking pictures or videos of students, to also include audio recordings.
- Updated the Young Person's Agreement to include reference to sexual harassment and making, creating or sharing images, videos or audio records of others without their consent (including through the use of AI).

Appendix A – Acceptable Use of Technology Policy for Staff

Acceptable Use of Technology Policy – Staff

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.

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.

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 IT 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.
- If I choose to use my personal mobile telephone or other device to access Trust or Academy IT systems such as email or Office 365 apps including Teams, I will ensure that adequate security is in place such as a device password, Touch ID or Face ID. I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to my line manager or appropriate person.
- I will respect security, and I will not disclose any password or security information to another person. I will use a strong password.
- I will never enter personal or sensitive data into an Artificial Intelligence tool (such as Chat GTP).
- I recognise that it is my responsibility to check the accuracy of any information generated by Artificial Intelligence tools and acknowledge that content generated by Artificial Intelligence may be incorrect, biased or inappropriate.
- I will immediately report any potential data breaches to the Principal/GDPR Nominated contact.
- I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of to the DSL as soon as possible.
- I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and other devices or websites.
- 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.

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 images or videos of adults or colleagues, unless I have permission to do so.

- I will not take pictures, videos or audio recordings of students on my personal devices and will never share images, videos or audio taken on work devices to the personal devices, personal online accounts or personal online storage belonging to myself or others.
- I will never be in possession of, or use, any form of covert recording equipment in the Academy or whilst representing the Academy at ay school activities or trips.
- 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 and the site guidance.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner only take place during official working hours.
- 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.
- All information discussed or received of a sensitive or confidential nature will remain so and only discussed with relevant key staff such as the Principal or DSL.

Ensuring safe and secure access to technologies:

- 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 and that they are protected by up-to-date security patches and anti-virus software and are free from viruses.
- I will not use personal email addresses for academy/Trust IT 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 IT 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 try to use any applications, such as VPN, that might allow them to bypass the filtering/security systems in place to provide a safe learning and teaching environment.
- I will not disable or cause any damage to school/academy equipment, or any equipment belonging to others.
- I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- 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.

Use of copyright resources:

- I will ensure that copyright resources are only used or shared with appropriate permissions. Copyrighted work will not be downloaded or shared including music and videos unless an exemption applies for teaching purposes.
- These purposes include:
    - the copying of works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes, it is accompanied by a sufficient acknowledgement, and the use is fair dealing. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but uses which would undermine sales of teaching materials are not;
    - performing, playing or showing copyright works in a school, university or another educational establishment for educational purposes. However, it only applies if the audience is limited to teachers, pupils and others directly connected with the activities of the establishment. It will not generally apply if parents are in the audience. Examples of this are showing a video for English or drama lessons and the teaching of music. It is unlikely to include the playing of a video during a wet playtime purely to amuse the children;
    - by recording a TV programme or radio broadcast for non-commercial educational purposes in an educational establishment, provided there is no licensing scheme in place. Generally, a licence will be required from the Educational Recording Agency;
    - making copies by using a photocopier, or similar device on behalf of an educational establishment for the purpose of non-commercial instruction provided that there is no licensing scheme in place. Generally, a licence will be required from the Copyright Licensing Agency.

These and other, exemptions to copyright are listed here: https://www.gov.uk/guidance/exceptions-to-copyright

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).

I have read and understood the above and agree that:

- I am responsibly upholding the requirements laid out above at all times and that even while in personal time I am representing the values and integrity of the school.
- 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
- I confirm that I have read and understood the Online Safety Policy and the Acceptable Use Policy

Signed:	
Name:	
Date:	

Appendix B – Acceptable Use of Technology Policy for Key Stage 1 Students

My name is _____

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone
12. I will not share my **PASSWORDS** with others

My trusted adults are:

_____ at school

_____ at home

For parents/carers.

We ask all children to sign an age-appropriate Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using technology. Please read and discuss this agreement with your child and then sign it. If you have any questions or concerns, please speak to [add name/job title].

You can find out more looking at the Academy's website and/or reading the Online Safety Policy and the Acceptable Use of Technology Policy. You can find support and online safety resources for parents at https://www.thinkuknow.co.uk

Parent name	Parent signature	Date

Appendix C – Acceptable Use of Technology Policy for Key Stage 2 Students

These statements can keep me and others safe and happy at school and home

1. ***I learn online*** – I use the school's internet, devices and logons for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I can't go to school***– I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher or a grown up at home.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
15. ***I say no online if I need to or want to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

16. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult, but very unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again. I do not keep secrets that are unsafe.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.
25. ***I know that the computer knows what I am typing and will report it to an adult if it is not safe***.

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult at school that includes _____

Outside school, my trusted adults are_____

	Parent/carer	Child
Name		
Signature		
Date		

For parents/carers.
We ask all children to sign an age-appropriate Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using technology. Please read and discuss this agreement with your child and then sign it, then ask your child to sign it.

You can find out more looking at the Academy's website and/or reading the Online Safety Policy and the Acceptable Use of Technology Policy.

You can find support and online safety resources for parents at https://www.thinkuknow.co.uk

Appendix D – Acceptable Use of Technology Policy for Key Stage 3-5 Students

We ask all young people and adults to sign an Acceptable Use of Technology Policy, which is a document that outlines who we expect them to behave when they are online and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on the academy site and outside).

We understand the importance of children and young people being able to use the internet for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times. Ensuring student safety online is a partnership between the student, their parents/carers and school and all have a role to play in it and need to work together.

This agreement is part of our overarching code of behaviour for children and young people and staff and volunteers. It also fits with our overarching online safety policy. If you would like to know more about this, please speak to your tutor or classroom teacher.

More information about online safety for parents is available from

- https://www.ceop.police.uk/safety-centre/
- https://www.thinkuknow.co.uk/
- https://educateagainsthate.com/parents/
- https://nationalonlinesafety.com/guides
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting
- https://www.internetmatters.org/
- https://www.net-aware.org.uk/
- https://www.childnet.com/resources/

Websites such as TikTok, Facebook, etc. are 13+ and YouTube is 13+ and 11+ with parental permission. Please find out more about this at https://nationalonlinesafety.com/guides. Please be aware that staff may direct students between the ages of 11 and 13 to YouTube videos for the purposes of learning. These will be age appropriate in content and by signing this agreement you are giving parental permissions for this.

More information about online safety for children and young people is available from

- https://www.thinkuknow.co.uk/
- https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/
- https://www.ceop.police.uk/safety-centre

Students: please read the following agreement and discuss it with your parents/carers.

Parents/carers: please read and discuss this agreement with your child and then sign it, then ask your child to sign it. If you have any questions or concerns, please speak to your child's tutor or classroom teacher.

Young person's agreement

1. I will treat myself and others with respect at all times. When I am online or using any device, I will treat everyone as if I were talking to them face to face.
2. I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access; the language I use and the information I share.
3. I will try to be positive and creative to learn and share, and develop new skills, and to have fun. I will make sure my use of technology does not harm anyone else.
4. I will only access age-appropriate websites, social media platforms, games and apps that are for school use.
5. I will not download copyrighted material (e.g. music, text, video etc.).
6. It can be hard to stop using technology sometimes. I will try to use it in moderation and not let it affect other areas of my life (such as sleep).
7. I will consider my online reputation with everything I post and share – I know anything I do can be shared and might stay online forever (even if I delete it). I understand that employers are increasingly searching applicants online, including social media accounts, and my activities online may impact negatively on my ability to get a job in the future.
8. I will not deliberately browse, download or upload material that could be considered offensive or illegal. This includes sites that encourage hate, sexual harassment or discrimination. If I accidentally come across any such material I will report it immediately to the school. If I am not in school, I will inform my parent/carer.
9. I will not send anyone material that could be considered threatening, bullying, offensive or illegal. Cyber bullying (along with all bullying) will be taken extremely seriously.
10. I will never take secret video, photos or recordings (including audio) of teachers or students, including during remote learning.
11. I will never make, create or share images, videos or audio recordings of others (including via Artificial Intelligence) without their prior permission and consent.
12. I will not give out any personal information online, such as my name, phone number or address.
13. I will not reveal my login, ID's or passwords to anyone and change them regularly. If someone else knows my passwords I will tell a teacher.
14. I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/carers and am accompanied by a trusted adult.
15. If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to a trusted adult. In school this might be [enter name].
16. I understand that my internet use at [Name of school] will be monitored and logged and can be made available to the school.
17. I will not try to bypass online security in any way or access any hacking files or tools. This is a criminal activity.
18. I will only access my own documents and files and not try to view, change or delete other people's files or user areas without their permission.
19. When learning remotely using Teams, teachers and staff will not behave any differently to when we are in school. I will do the same.
20. I will only use personal devices in school if I have permission to do so.
21. I understand that it is illegal to possesses, distribute, show and make any naked image or vide of anyone under 18, including of myself. This includes printing and viewing or 'downloading'. I understand that staff can search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
22. I understand that the computer systems are recording the keystrokes that I am typing. This will be reported to an adult if it is not safe.
23. I understand that when I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand the work of others may not be truthful and may be a deliberate attempt to mislead me. This is particularly important when using Artificial Intelligence, as it may produce information that is incorrect, biased or unsuitable.

Online Learning (Microsoft Teams)

Brooke Weston Trust and (School name) uses Microsoft Teams as the learning platform providing communication to staff classes and student groups.

I agree that:

- I will use Microsoft Teams and other authorised websites (for example Hegarty Maths, Seneca Learning) to complete learning activities.
- I will ensure that all work uploaded or files sent will be appropriate.
- I will only use the chat function to contact my teacher if I need help with the work set. If this is required, I understand that this needs to be appropriate.
- I will limit the use of the chat functionality with other students, and when used will make sure that it is appropriate as records are kept of all chats.
- I will not use the video functionality. If needed, and requested to by a member of staff, I can activate my microphone to talk but must be appropriate.
- I understand that lessons/video communication is recorded for safety.

I understand that these rules are designed to keep me safe and that if I choose not to follow them, school staff may contact my parents/carers.

Signatures:

We have discussed this online safety agreement and agree to follow the rules set out above.

	Parent/carer	Young person
Name		
Signature		
Date		

Appendix E – Staff log of remote learning lesson contacts and issues

Staff name and role	Other staff present (if a live video, stream or chat)	Name of class, group or individual	Time and frequency	Scheduled? (Y / N)	Platform used. Teams!	Issues, worries, concerns (technical, safeguarding, DP or other) and general trends. One-to-one conversation summarised on CPOMS

APPENDIX F: INDIVIDUAL PUPIL RISK ASSESSMENT FOR REMOTE MEETINGS ONLINE

The purpose of this risk assessment is to document the risk factors for the named student and what measures are in place to manage them so that a 1:1 meeting via Teams can take place as safely as possible. A copy of this MUST be stored on CPOMS along with the outcomes of the meeting.

Pupil's Name: **Year Group:** **Date:**

What causes concern? •	What health and safety hazards could arise? •
What support has already been put in place? •	Which activities <u>cannot</u> be safely managed, as far as it is possible to foresee? •

Activity	Risk Factor	Counter measure	Comments/actions	Risk factor with measures in place	Consequence of failure to meet this requirement

Staff Member:

Signed:

Principal (or delegated person):

Signed: