Acceptable Use Agreement - Brighter Futures Learning Partnership Trust - Staff - Version 5

This agreement is for Staff, support staff, governors, visitors, wider stakeholders with access and external contractors.

When using the Trust IT systems and accessing the internet, or offsite on a work device:

- I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature.
- I will not use Trust IT systems in any way which could harm the school, college, or Trust's reputation.
- I will not access social networking sites or chat rooms unless for educational purposes.
- I will not attempt to bypass the internet filtering or Trust/School IT security.
- I will not use any improper language when communicating online, including in emails or other communication systems.
- I will only use Trust IT systems, external logins, and email for school related purposes. Other use will be with the permission of Trust IT Department.
- I will not divulge any Trust or School related passwords and I will comply with IT security procedures and Data Protection policies.
- I will comply with the Trust's multi-factor authentication (MFA) requirements. Where required, I understand that this may include the use of an authenticator application on a personal device when not on school/UTC premises, and I will ensure any device used for this purpose is appropriately secured and that any loss or compromise is reported immediately to the Trust IT Department.
- I will make sure email and social media interactions with staff, parents, students, and members of the public are responsible and in line with the Social Media, Safeguarding and Digital Safety policies.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to students or parents.
- I accept that students and parents may find these details out, and that any contact should be logged and either not reciprocated or replied to in line with Trust policies.
- I will not use personal accounts for Trust or school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Policy.
- I will follow Trust/school policy regarding external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations. Any software requests will be made to the Trust IT Department.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory, or copyright infringing.
- Photographs of staff, students and any other members of the school and Trust community will not be used outside of Trust/School systems unless written permission has been granted by the subject of the photograph or their parent/guardian (where the subject is below the age of 18).
- I will ask the permission of the Head Teacher/Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and internet activity is logged and monitored and that the logs will be made available to Trust Leaders or School Senior Leaders in the event of allegations of misconduct.
- I will take all reasonable steps to ensure that work devices are secure, password-protected, and encrypted when using them outside school, and keep all data securely stored in accordance with this policy and the Data Protection Policy.
- I will inform the designated safeguarding lead (DSL) and Trust IT manager if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will champion the Digital Safety Policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will ensure the Trust IT team is made aware of all IT issues.
- I will follow all cyber security recommended practices outlined in the Digital Safety Policy.
- I will complete all mandatory IT training in line with cyber security and data protection as required.
- I have read and will comply with the Social Media Policy, Digital Safety Policy and Artificial Intelligence Policy.

Use of Artificial Intelligence (AI)

- I will comply fully with the Trust's Artificial Intelligence (AI) Policy.
- I will not input, upload, or share personal data, confidential information, safeguarding information, or sensitive Trust data into any AI system unless explicitly authorised and risk assessed.
- I understand that AI-generated content remains my professional responsibility and I will verify its accuracy, appropriateness, and compliance with safeguarding, copyright, and data protection requirements before use.
- I will not use AI tools in a way that could compromise assessment integrity, professional standards, or safeguarding expectations.
- I will not use AI to create content that could be considered harmful, discriminatory, misleading, or inappropriate.

Data Protection and GDPR

The Data Protection Act 2018 and the GDPR legislation effective from 25th May 2018 states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices that are owned by the school or Trust, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- Avoid transferring data where possible. Where the transferring of data is necessary the user must use appropriately encrypted and secure means.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- This is only done for specific purposes with regards to providing these to a 3rd party where we have performed a Data Protection Impact Assessment (DPIA) and a formal agreement in place (for instance examination boards).
- You should never physically transport personal data for other purposes where you can digitally share the data within our pre-existing systems (for example OneDrive or SharePoint).
- the data must be encrypted, and password protected.
- When storing on a portable device the device must be owned by The Trust or School and must be secured by the IT Department including a password and encryption.
- Data on removable media must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected).
- the data must be securely deleted from the device once it is no longer required.

Signed	
Employed at School	

Date	