# ICT Acceptable Use Policy

# Trust Mission Statement

Our mission is to create high quality educational opportunities for all children and young people across the partnership by developing a strong collaborative and co-operative model through which we encourage autonomy, share best practice, enhance the professional aspirations of our staff and ensure the safety and well-being of all pupils and staff.

# Contents

## Linked Documents

- Staff Code of Conduct
- Disciplinary Policy
- School E-Safety Policy
- Remote Learning Policy
- Child Protection Policy
- Health & Safety Policy
- GDPR Policy

## 1.0 Introduction

1.1 The Trust promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, and wish to support staff in ensuring that technology is used appropriately.

1.2 This acceptable use policy is designed to outline staff responsibilities when using technology, whether this is via school devices or personal devices, on/off the school premises.

1.3 All staff and workers are expected to comply with this policy and understand it in detail.

## 2.0 Scope & Principles

2.1 This policy applies to all employees at Bradgate Education Partnership.

2.2 This policy should also be read in conjunction with the Trust's Remote Learning Policy, the Trust's Code of Conduct and GDPR Policy.

2.3 The Trust operate an Office 365 system and it is expected that all employees only use this system for communication purposes eg. Outlook/Microsoft Teams unless it has been expressively agreed with the Trust

## 3.0 Using Technology in School

3.1 Staff will only use ICT systems, such as computers including laptops and tablets, which have been permitted for their use by the Head Teacher.

3.2 Staff will only use the approved email accounts that have been provided by the Trust.

3.3 Staff will not use personal emails to send/receive/manage personal data or information.

3.4 Staff will comply with their obligations in relation to data protection and GDPR requirements and will only share/store sensitive personal data with staff/3rd parties as and when appropriate in line with professional duties.

3.5 Staff will where it is possible, delete any chain letters, spam and other emails from unknown sources without opening them.

3.6 Staff will ensure they obtain learning materials from approved sources.

3.7 Staff will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet on school based devices.

3.8 Staff will not share school-related passwords with pupils, staff or third parties unless permission has been given to do so.

3.9 Staff will only install software onto school ICT systems when they have sought permission from the IT Network Manager, Estates & IT Manager or the Head Teacher.

3.10 Staff will only use school removable devices and where this is the case, limit use of removable devices and where they are used they will be used with encryption for the purpose of photocopying or scanning and store all pupil data securely on the schools' SharePoint platform.

3.11 School owned removable media will be returned to either the Head Teacher or the ICT Network Manager/Estates & IT Manager for safe disposal once they are finished with it.

## 4.0 Mobile devices

4.1 Staff will only use school-owned mobile devices for educational purposes should it be required

4.2 Staff will only use personal mobile devices during out-of-school hours, personal use is permitted on personal devices during break and lunch times.

4.3 Staff will ensure that use of mobile devices follow local procedures outlined by the Head Teacher.

4.4 Staff will not use personal mobile devices to take images or videos of pupils or staff – and will seek permission from the Head Teacher before any school-owned mobile device is used to take images or recordings.

4.5 Staff will not use mobile devices to send/publish inappropriate messages/content/images or recordings.

4.6 Staff will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

4.7 Staff will not access the WiFi system using personal mobile devices, unless permission has been given by the Head Teacher or ICT Technician.

4.8 Staff will not use personal mobile devices to communicate with pupils or parents.

4.9 Any contact with parents/pupils must take place on school approved mobile devices permitted by the Head Teacher.

4.10 Staff must not store any school data on a personal mobile device.

## 5.0 Social media and online professionalism

5.1 Where staff are representing the school online or on social media, e.g. through blogging/Twitter/Facebook, they will ensure that they act professionally at all times, only express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.2 Staff will only use any school-owned mobile devices to access social networking sites to the benefit of learning or material being taught; staff will gain permission from the Head Teacher before accessing the site.

5.3 Staff will not communicate with pupils or parents over personal social networking sites and if they are contacted by parents/carers via social media they must inform the Head Teacher of this

5.4 Staff will ensure that their own personal social media accounts have the appropriate privacy settings in place so that parents/carers and pupils can't access them – staff will not accept friend requests.

5.5 Staff will not publish any comments or post about the school/Trust on their social networking sites which may affect the school/Trust reputation.

5.6 Staff will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.

5.7 Staff will not give their home address, phone number, mobile number, social networking details or email addresses to pupils or parents/carers – any contact with parents will be done through authorised school contact channels.

## 6.0 Training

6.1 Staff will ensure they participate in any e-safety or online training offered.

6.2 Staff will ensure they will employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

6.3 Staff will ensure that they deliver any training to pupils as required.

## 7.0 Reporting misuse

7.1 Staff will ensure that they adhere to any responsibility they have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.

7.2 Staff will ensure that they report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the Head Teacher.

7.3 Staff understand that their use of the school internet and work devices will be monitored by the Trust and recognise the consequences if they breach the terms of this policy.

7.4 Staff understand that the Head Teacher may decide to take disciplinary action against them in accordance with the Trust's Disciplinary Policy, if they are in breach of this policy.

## 8.0 Using technology for the purpose of remote learning

8.1 Staff will only communicate with pupils using pre-approved technologies and communication platforms approved by the Trust/Head Teacher – the main communication tool being Microsoft Teams with pupils, parents/carers.

8.2 Staff will use a mixture of live and pre-recorded communication/teaching methods for remote learning.

8.3 Staff will ensure that the 'chat' functions that are enabled within Microsoft Teams are used appropriately addressing any issues that may arise.

8.4 Where recording of meetings/recording of live learning is taking place, staff must make pupils, parents/carers aware that this is the case so they are fully aware that their participation may be recorded.

8.5 Staff must also ensure that any pupils being used to participate in the delivery of remote learning, consent is received prior from parent/carer

8.6 Staff will ensure that they monitor the use of remote learning platforms and will report any e-safety concerns regarding uploaded pupil content or inappropriate use of the learning platforms on CPOMS under the category of 'E-Safety'.

8.7 Where a 1:1 remote learning/tutoring online is required, staff will seek approval from the Head Teacher first.

8.8 Staff when using technology for extended periods, will follow the guidelines of the DSE (Display Screen Equipment) DSE Guide: https://www.hse.gov.uk/msd/dse/

## 9.0 Using technology for the purpose of remote learning from home

9.1 In the exceptional circumstances where staff need to undertake remote learning from home they need to be supported to do so appropriately and safely

9.2 Staff should ensure their background to their remote learning is professional eg Microsoft Teams background is set/resources set up in the background/plain screen background

9.3 Staff should ensure that if family members are present within the home setting, access/overhearing of information is only appropriate and nothing confidential is shared

9.4 Staff should ensure that they are only using school/Trust devices

## 10.0 Support

Where staff require support with use of ICT or remote learning they must contact the ICT Technician in place for the school or the Head Teacher.