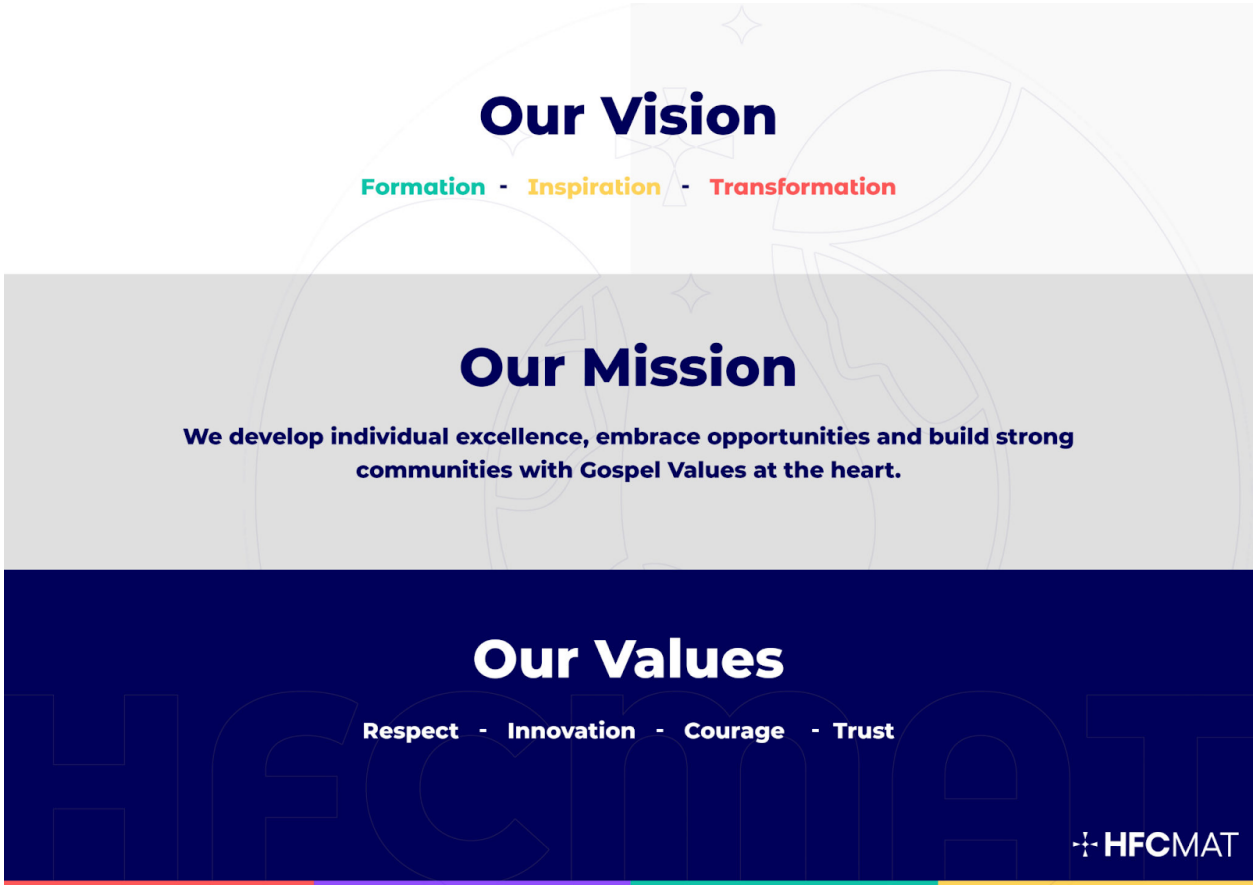
Acceptable Use of IT Policy



Document Management

Policy name:	HFCMAT Acceptable Use of IT Policy		
Approved by:	HR & Pay Committee	**when:**	Autumn 2022
Review by:	Operations Manager	**when:**	Autumn 2024
File location:			
Version control:	New March 2022 v1		

Acceptable Use of IT policy

1. Introduction and aims

IT is an integral part of the way our Trust works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of our schools.

However, the IT resources and facilities our Trust uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

This policy covers all users of our Trust's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policies and staff code of conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- 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 2018
- Searching, screening and confiscation: advice for schools

3. Definitions

- **"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

- **"Users":** anyone authorised by the Trust to use the IT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the Trust to perform systems administration and/or monitoring of the IT facilities
- **"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

4. Unacceptable use

The following is considered unacceptable use of the Trust's IT facilities by any member of the Trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's IT facilities includes:

- Using IT facilities to breach intellectual property rights or copyright
- Using IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust or school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the Trust and/or school, or risks bringing either into disrepute
- Sharing confidential information about the Trust, school, its pupils, or other members of the school community
- Connecting any device to the IT network without approval from authorised personnel
- Setting up any software, applications, the use of web-based programs or web services on the school's network without approval by authorised personnel or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data. Approval needs to be given in the schools IT Change Management meeting.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust or school's IT facilities
- Causing intentional damage to IT facilities
- 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
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust

- Using websites or mechanisms to bypass the Trust and school's filtering mechanisms

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Executive Headteacher and local SLTs will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's IT facilities.

4.1 Exceptions from unacceptable use

Where the use of Trust IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

This will need to be obtained in written form from the respective headteacher.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the specific school's policies for behaviour and staff conduct.

This may include the removal of access or specific functions of IT provision, as decided by the SLT IT lead in the specific school.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to Trust IT facilities and materials

Mercu manages access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

- Computers, laptops, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact Mercu

5.1.2 Online Live Lessons

Staff across the trust may be required to deliver remote lessons online. This policy will apply to the use of facilities and materials to conduct these. The running of such sessions is covered by Appendix 6.

5.1.2 Use of phones and email

The school may provide each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must 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.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform Mercu immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business unless given written permission to use a personal device by the Headteacher of their respective school. In this rare instance, staff must call with their number being withheld if using to contact parents or families of the school.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out in section 4.

The school will not record in-coming and out-going phone conversations.

5.2 Personal use

Staff are permitted to occasionally use school IT facilities for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused. The School Business Leader (SBL) or Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust's Online Safety and Mobile Phone Policy to access Trust and school cloud infrastructure as long as this does not constitute 'unacceptable use', as defined in section 4.

Staff should be aware that personal use of IT (even when not using school IT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook and social media accounts (see appendix 1).

5.3 Remote access

The Trust operates a cloud-based IT solution. All documents, interactions, communication and participation within this solution is deemed to be IT facilities of the Trust. All files and data within the online environment are deemed to be materials covered by this policy.

We allow staff to access the other parts of some school's IT facilities and materials remotely.

Staff accessing the school's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and take such precautions as Mercu may require from time to time against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

Schools in the Trust have official Facebook, Twitter and Instagram pages. These are managed by staff members who have been authorised to manage, or post to, the account. Those without such permission must not access or attempt to access the account.

The Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of IT facilities

The Trust reserves the right for the central team and each school to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised IT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

Each school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards

- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to IT facilities

The Trust will oversee the procurement of all equipment purchases for each school to ensure consistency in product across all schools. The access granted to students to use these facilities will be at the direction of each school's SLT and the rules they set out relating to use of specific rooms, locations and equipment during the school day, after hours and off site.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3 Unacceptable use of IT and the internet outside of school

Schools will sanction pupils, in line with their respective behaviour policy, if a pupil engages in any of the following **at any time**:

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities
- Causing intentional damage to IT facilities or materials
- 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
- Using inappropriate or offensive language

Sanctions for misuse will be decided upon by following the respective school's behaviour policy.

7. Parents

7.1 Access to IT facilities and materials

Parents do not have access to the school's IT facilities as a matter of course.

However, parents working for, or with, the Trust or a school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Parents must not use pupil accounts to communicate with staff in the trust. They need to use appropriate communication channels as set out by each individual school. This is likely to be using the parent's own email address to email the relevant member of staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's IT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the Trust IT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords are required to be updated by all users once every 3 months to provide enhanced security.

Password resets will only be processed when it is verifiable that the owner of the account is requesting this. When a student is not on site and requires a reset each school will have a specific protocol for doing this to ensure data protection legislation is followed.

8.2 Software updates, firewalls, and anti-virus software

All the Trust's schools' IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's IT facilities.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the Trust's IT facilities will have clearly defined access rights to the Trust and specific school systems, files and devices.

These access rights are managed by each school's IT support.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert IT Support immediately.

Users must always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The Trust and schools ensure that its devices and systems have an appropriate level of encryption. USB memory sticks should not be used. All documents should be accessed and saved using Google Workspace.

School staff may only use personal devices to access school data, work remotely, or take personal data (such as pupil information) out of school if they are unable to access and use the approved Google Workspace cloud environment and have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by IT support.

9. Internet access

Each school internet connection and wifi network is secured. The internet is filtered with high level restrictions on what can and cannot be accessed. The IT Support team monitors the functioning of this. Should a specific site appear to any staff as being inappropriate, they must notify IT support and the School Business Lead.

9.1 Pupils

Pupil access to Wi-Fi in schools across the trust will be managed by individual guidelines relevant to their context

9.2 Parents and visitors

Parents and visitors to a school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The Headteachers, Trust SLT and local school SLT monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

11. Related policies

This policy should be read alongside the:

- Online Safety and Mobile Phone Policy
- Child Protection and Safeguarding Policy
- Behaviour Policy
- Disciplinary and Capability Procedure
- Code of Conduct
- Trust Data Protection Policy

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook and social media platforms

1. Change your display name for personal accounts– use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils/employer
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Do not activate desktop or browser notifications on a work device as this may interfere with the delivery of a lesson

---

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Email/text for parents (for school announcements and information) ● School communication apps (Eg:Parent Mail)	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: ● Be respectful towards members of staff, and the school, at all times ● Be respectful of other parents/carers and children ● Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: ● Use my child's school account (including email and Google Workspace) to attempt to communicate with the school, I will use the approved communication avenues to contact staff (eg email, phone call, APPS) ● Use private groups, the school's Facebook page, community facebook pages , whatsapp or personal social media to complain about or criticise members of staff or the school. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way ● Use private groups, the school's Facebook page, whatsapp or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident ● Upload or share photos or videos on social media or via text message/whatsapp of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

<table>
<tr><th colspan="2">Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When using the school's IT facilities and accessing the internet in school, I will not:
● Use them for a non-educational purpose
● Use them without a teacher being present, or without a teacher's permission
● Use them to break school rules
● Access any inappropriate websites
● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
● Use chat rooms that are not authorised by the school
● Open any attachments in emails, or follow any links in emails, without first checking with a teacher
● Use any image of another student or member of the public as my profile picture
● Use any inappropriate language when communicating online, including in emails
● Share my password with others or log in to the school's network using someone else's details
● Bully other people
I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's IT systems and internet responsibly.
I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 4: Acceptable use agreement for younger pupils

<table>
<tr><th colspan="2">Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's IT facilities (like computers and equipment) and get on the internet in school, I will not:
● Use them without asking a teacher first, or without a teacher in the room with me
● Use them to break school rules
● Go on any inappropriate websites
● Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
● Use chat rooms
● Open any attachments in emails, or click any links in emails, without checking with a teacher first
● Use unkind or rude language when talking to other people online or in emails
● Share my password with others or log in using someone else's name or password
● Bully other people
I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.
I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.
I will always be responsible when I use the school's IT systems and internet.
I understand that there will be consequences in line with our behaviour policy if I do certain unacceptable things online, even if I'm not in school when I do them.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's IT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's IT facilities and accessing the internet in school, or outside school 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 (or create, share, link to or send such material) ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software, or connect unauthorised hardware or devices to the school's network ● Share my password with others or log in to the school's network using someone else's details ● Share confidential information about the school, its pupils or staff, or other members of the community ● Access, modify or share data I'm not authorised to access, modify or share ● Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and IT manager know if a pupil 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 always use the school's IT systems and internet responsibly, abiding by the HFC IT and Acceptable Use policy, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Online Live Lesson Acceptable Use Policy (AUP)

Leadership Oversight and Approval

Remote learning will only take place using Google Classroom. Google Classroom has been assessed and approved by the Trust central IT teams, the Headteacher and the Senior Leadership Team (SLT).

Staff will only use school accounts with learners and parents/carers. Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.

Staff will use work provided equipment where possible. e.g. a school laptop, tablet or other mobile device.

Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by the specific school SLT

All remote lessons will be formally timetabled; and scheduled in the specific class channel. Another colleague can be invited to support in the lessons. School leaders are able to be invited and should be able to drop in at any time.

Live streamed remote learning sessions will only be held during the agreed and published times by the SLT.

Data Protection and Security

1. Any personal data used by staff and captured by Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with the Trust's data protection policy.
2. All remote learning and any other online communication will take place in line with current Trust confidentiality expectations as outlined in Trust policies
3. All participants will be made aware that Google Classroom may record activity and that remote lessons are being recorded and stored on the School Google Workspace platform.
4. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
5. Only members of the HFCMAT community will be given access to Google Workspace.
6. Access to Google Workspace will be managed in line with current IT security expectations as outlined in the Trust IT Security policy.

Session Management

1. Staff will schedule and ensure the correct class, time, and date of any sessions held are done using the correct method in Google Classroom for their class.
2. Appropriate privacy and safety settings will be used to manage access and interactions.
3. When live streaming with learners:
    - contact will be made via learners' school provided email accounts and subsequent Google Classroom login.

- staff will ask the student to disable their video/mute their microphone at their discretion. Staff are able to remove the student from the lesson if they do not follow instructions.

4. It will be at the lead teacher's discretion if they would like students to use their camera later in the lesson to see students. This will be done by reminding students to be appropriately dressed and to use a blurred or picture background. Lessons will be recorded to safeguard all involved.
5. Live 1 to 1 sessions can take place with approval from a member of the SLT.
    - In this scenario a parent/carer is to be present in the room and a 2nd member of staff on the call. If this is not possible, the session must still be recorded.
6. Access links are not to be made public or shared by participants.
    - Learners and/or parents/carers must not forward or share access links.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first who will seek permission from a member of the SLT.
7. Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

Behaviour Expectations

1. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
2. All participants are expected to behave in line with existing local school policies and expectations.
3. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
4. When live streaming, participants are required to:

- Ensure student cameras are to be switched off (at the teacher's/leader's discretion)
- Wear appropriate dress in case of a camera being accidentally turned on
- Check that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

All Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

Participants are encouraged to report concerns during remote sessions:

1. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated and concerns will be recorded on ARBOR/ CPOMS, reported to the line manager/HOD and DSL if a safeguarding concern.
2. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

- Sanctions for deliberate misuse may include, restricting/removing use, contacting police if a criminal offence has been committed.

3. Any safeguarding concerns must be reported to Designated Safeguarding Leads via CPOMS, in line with local schools Safeguarding policy.

Appendix 7: Online Live Lessons Acceptable Use Agreement

As we introduce the use of Google Classroom to run online lessons, it is important that all students are aware of the way they need to conduct themselves in this new way of working. Below are the main points that need to be followed to ensure that learning is productive in this new way of working.

All lessons will be recorded for safeguarding purposes. By entering the lessons, you agree to this recording.

What we ask of you:

- Be ready to start your lessons on time.
- Be polite to our teachers and friendly to other learners.
- If you have something you would like to contribute or ask, type in the chat box, your teacher will invite you to unmute if needed. The chat function is for learning-based comments or questions, not a social area.
- Respect other people's opinions and ideas.
- Always try your best in all that you do.

Display safe online behaviour:

- Please switch your camera off before entering the lesson.
- Be appropriately dressed. Just in case your camera turns on accidentally.
- Do not give your personal contact details to anyone else in your online class.
- Remember everything you do on the internet can be seen by someone else.
- Ignore inappropriate online behaviour by others, our teachers will deal with this.
- Be responsible for everything you do and say online.

Our teachers will not tolerate:

- Bullying including discriminatory, offensive, aggressive or unpleasant language or threats. All are unacceptable – this may result in removal from our classroom.
- Abuse of your microphone - this will result in your microphone being muted.
- Abuse of the chat box – this may result in you being removed.
- Students should not record the lesson on your device or any other device.

Remember:

All lessons are recorded.