Hodge Hill College

Acceptable Use Policy Staff

Approved On/By:	Finance, Staffing and Premises Committee
Last Reviewed On:	21th November 2023
Next Review Due By:	FSP Autumn Term 2024
Monitoring & Review:	Annually
Staff Member(S) Responsible:	Mr D Abbas – ICT Manager

New technologies have become integral to the lives of staff and children in today's society. The Internet and other digital technologies are powerful tools, which open new opportunities for everyone. These technologies stimulate lessons to promote effective learning. All users have an entitlement to a safe working environment at all times.

This Acceptable Use Policy is to ensure:

- that staff and volunteers will be responsible users and stay safe when using the digital technologies for their professional use.
- that the school ICT infrastructure and users are protected from accidental damage or misuse that could put all users at risk
- that all users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that all users have access to ICT facilities to enhance their work and learning opportunities. All staff/pupils must be responsible users and adhere to all policies at all times.

Acceptable Use Policy Agreement

I understand that I must use the school ICT systems in a responsible manner, ensuring that there is no risk to my safety or any other users. Where possible I will educate the pupils in my care in the safe use of technologies and enforce the e-safety policy and Data Protection Policy.

Professional and personal safety

- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school.

- I understand the school ICT system is used for professional educational use.

- I will not disclose my account credentials to any other colleague, nor will I use any other colleague's credentials.

- I will report any issues, inappropriate/harmful material to the ICTS department immediately.

- I understand it is my responsibility for locking my workstation or any other portable device and making it secure when I am away from my desk. In addition, at the end of each day I will shut down my Computer and any other IT equipment. Under no circumstances must I leave any sensitive or confidential information on my screen or desk area.

Communication

- I will not access or modify any other user's files
- I will communicate with other staff members in a professional manner. I will not use inappropriate language and I will respect others may have different opinions.
- I will not misuse the e-mail system. If I observe any inappropriate use I will contact Team ICTS.
- I will ensure that when I take images of pupils/staff and/or publish images using school owned devices, I will seek their permission by checking consent using SIMS, if no permission is given then no photograph(s) will be used, at all times you must adhere to any school policy relating to the use of photographs. I will not use my personal equipment to take these images.
- I will only communicate with staff/pupils using official school systems.
  Any such communication will be conducted in a professional manner.
- I will not engage in any communication that may compromise my professional duties

Safe environment

- When using any technologies in school I will follow all practices listed in this agreement and abide by other ICT related and Data protection Policies
- I will not access or use my personal e-mail account for my professional duties.
- I will only open email attachments from trusted stakeholders to reduce the risk of viruses
- Do not send attachments internally, but instead use a hyperlink to the document on the school staff shared drive
- I will not upload/download any inappropriate material which may cause harm, offence or distress to other stakeholders
- I will not download any material/content that is not from a trusted party. Any software downloads need to be approved by the ICTS department
- I will not cause any damage to the school ICT equipment.
- I will only disclose information about myself and others in accordance to the data protection policy and other policies relating to sharing data (Privacy Notice).
- In accordance with the Data Protection Policy all Staff and Pupil information is stored securely at all times
- All external emails are filtered and managed by our internal policies and the Office 365 platform prior to being received.
- I will immediately notify the appropriate member of staff if I observe any damage, defect or health and safety issue
- When using any Social Networking sites I will ensure that the privacy settings are set correctly and only post professional content.

Information Security and Data Protection Tips for School Staff

- I will ensure that I have copyright permission to use the original work of others prior to using it in my own work. I will not distribute any files/folders without the prior consent of the owner.
- I understand that I must only use YouTube to play videos for Classroom resources.

- I understand that all users will be notified of the Acceptable Use Policy via a logon screen, which will appear whenever a user logs on. To proceed, users will have to click on a button to accept the conditions. In addition, all workstations used at Hodge Hill College are monitored by Impero Software at all times.
- When using services offsite such as FoldR and Emails, I must ensure that no files are downloaded to my personal device.
- Please ensure that any school portable equipment (mobile phone, iPad and laptop) has the appropriate security such as PIN codes and passwords configured.

Hardware

- For any school laptops, tablets, phones and USB memory sticks must be encrypted if they are used to process personal data, regardless of whether the contents are sensitive information or not
- The school does not permit the use of personal memory sticks don’t be tempted to use them “just this once” as if it results in a data breach it may be considered a serious disciplinary offence

Software

- You must regularly connect your school laptop to the school wi-fi network to perform and complete relevant updates.

Passwords & Security

- Use passwords that have at least 8 characters and contain mixture of upper- and lower-case letters, numbers and characters
- Use different passwords when accessing sensitive documents or storage locations
- Lock your computer when you are logged on and leaving it unattended

Email

- Only use a school email address to process personal information and be mindful of “conversations” when replying to emails in case there is personal data included in the email trail of previous messages. Images of Pupils cannot be sent in an email
- Ensure personal data is not included directly in email text or any attachment when sending messages outside the school’s own network.
- Under certain circumstances, you may need to send an attachment containing sensitive information to a third-party agency. These attachments must be encrypted using the built-in encryption process. The attachment must be a zipped file which is password protected.
- Do not send attachments internally, but instead use a hyperlink to the document on the school staff shared drive
- Be aware of synchronising phones and tablets to cloud storage as documents, photos and emails could be saving automatically to the cloud
- Remember that if you look at a PDF file it usually downloads the file to the device you are using and may be automatically backed up to cloud storage without you realising
- Don’t add your school email account in the generic mail app on your personal phone/device

Personal Information

- Do not access, create or save files that contain personal information on a personal device or cloud storage area
- Keep all paper and electronic files that contain personal information safe, secure and away from anywhere other people can easily access them
- Dispose of paper and electronic files in line with appropriate retention schedules, along with any redundant IT equipment that contains personal information inline with school policy and never throw it away in the bin
- Do not display unnecessary personal information around school unless there is valid reason or prior consent has been obtained
- Always ensure people requesting personal information about other people are who they say they are, and have either a valid reason or consent from the data subject to receive that data
- Staff should only access pupil data/personal information in school or a school laptop
- Staff should only access staff personal information for e.g. performance management documentation or observation sheets should only be accessed in school or a school laptop

Responsibility

- I understand that this Acceptable Use Policy applies to the use of school ICT equipment and systems in school, but also applies to my use of schools ICT systems outside of school for the following services Emails, Website, FoldR and any other school portal/resources.
- All ICT equipment such as laptops, iPads and mobile phones etc. must be stored securely onsite at all times.
- I understand I must adhere with this Acceptable Use Policy Agreement and failing to do so could be subject to a disciplinary action.
- All loaned ICT equipment will need to be signed for. You manage the equipment and are held responsible until the end of the loan.

Internet Use Policy

Hodge Hill College has a policy for the use of the Internet that all employees must ensure that they:

- Comply with the current policies and practices
- Use the Internet in a professional and acceptable way at all times
- Never misuse the Internet in a way that may cause harm to an employee or business

Monitoring

- All Internet data that is transmitted and/or received by Hodge Hill College computer systems is considered to belong to Hodge Hill College and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties

- The Internet usage for all users is managed and monitored by Hodge Hill College. We reserve the right to monitor Internet traffic, and access data if there is an observation of misuse.
- All sites/downloads are monitored by Hodge Hill College if they are deemed to be harmful or identified not to be productive for the business.
- As an employee, if you are a suspect of harmful content please consult the ICT Operations Manager.

Unacceptable Behaviour

The following is deemed unacceptable use of Behaviour by Employees:

- Using the Internet to post discriminatory, harassing or threatening messages or images about other employees or personnel that may be found defamatory to Hodge Hill College
- Perpetrate any form of fraud
- Disclose another employees account credentials
- Downloading, copying software or electronic files that are copyrighted
- Sharing confidential information such as Pupil/Staff information should be restricted to authorised personnel only and with authorised 3rd parties such as agencies and other schools. Throughout the whole process the GDPR regulations must be adhered to.
- Accessing inappropriate sites or some form of harmful content.
- Revealing confidential information about Hodge Hill College in an open public website e.g. financial information
- Introducing any form of harmful content such as software

If an employee is unsure about any part of this policy, then he/she should liaise with the ICT Operations Manager for further guidance.

All employees or temporary staff who have authorised access to use Hodge Hill College Internet services are required to this agreement confirming their understanding and acceptance of this policy.

Email Policy

This policy applies to all staff using the Electronic Mail system both web-based and using the Outlook client software during employment at Hodge Hill College. Every member of staff has the responsibility to adhere to the following policy and procedures.

Email is a business communication tool, and all users must use this tool in a responsible and professional manner. Hodge Hill College reserves the right to inspect the contents of any emails sent or received by employees.

Use of E-mail

- The primary use of the email system is for business. Only in approved circumstances can it be used for personal use.
- There may be an occasion/situation where you need to email sensitive documents to an approved authorised 3rd party after all other options have been exhausted. Any Email attachments sent externally containing sensitive information (staff/pupil personal details) must be password protected and encrypted at all times. In addition, no personal information (first name, form group etc...) about staff or pupils should be entered into the subject line of any email.
- An email system provides a fast form of communication. When sending emails ensure that the information is accurate, conforms to the netiquette rules and has been proof read prior to sending them. If an email is found to contain offensive, defamatory, obscene or racist references, yourself and Hodge Hill College can be held liable.
- Email messages may contain harmful content. If you send an email that contains a virus, yourself and Hodge Hill College can be held liable. Under no circumstances must you open emails and/or attachments from an unknown sender, if unsure please contact the ICT Operations Manager.
- All personal/confidential information should not be sent without the understanding that it may be intercepted during transmission. Please ensure that the intended recipient email address is correct. The consequence of an email being received by an unauthorised recipient could lead to a civil penalty of up to £500,000 from the Information Commissioner Officer (ICO).

Hodge Hill College considers email as an important method of communication and understands the importance of ensuring every email account consists of the correct content and speedy replies to convey a professional image and to deliver good customer service.

Therefore, Hodge Hill College would like staff to adhere to the following procedures.

Good Practice for Managing E-mails

Creating and Sending/Receiving Emails

1. Staff are prohibited from sending inappropriate content or content deemed to be harmful.

2. Emails should be sent to recipients that legitimately need to read the email. Forwarding unnecessary emails can overload the system. If you need to send an attachment to an external agency as a last resort, please ensure that the attachment(s) are less than 50MB in size and are password protected and the email has been sent in an encrypted manner. Do not send attachments internally but instead use a link to the document on the school staff shared drive

3. All emails reflect on Hodge Hill College image and reputation. Email messages must always be appropriate, professional and include the approved signature with branding. (Please see sample email on page 9).Prior to sending/forwarding emails with attachments, ensure you have permission from the owner, as you may be liable for copyright infringement. If in doubt, please contact the ICT Operations Manager.

4. Staff are not authorised to retrieve or read any email messages not intended for them. In certain circumstances, there may be a requirement to access your email e.g. Long-term sickness. At which point we would seek approval from the Head Teacher or Business Manager.

5. Prior to sending an email, ask yourself is this the best form of communication for the content. *'Would a Telephone conversation / face to face be the preferred option?'*

6. Any attachment that you are required to retain should be in accordance to the Data Retention guidelines. Attachments should be saved securely on the Hodge Hill College system(s). The email can then be deleted, dependent upon email message content.

7. Staff must proof read all emails before sending and comply with the following sending rules;

   - Do not use text language or informal language in school e-mails.
   - Always ensure that your signature is present with the appropriate branding and contact details.
   - Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
   - Never write a whole e-mail in capital letters. This can be interpreted as shouting.
   - Always spell check an e-mail before you send it. Do not use the urgent flag unless it is necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.

- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

8. To minimise the stress of the volume of email messages, please ensure you manage your emails by filing and deleting them accordingly.

Managing Emails and accounts

1. Under no circumstances should the school email system be used for anything other than for business use.
2. Hodge Hill College confidential emails should be distributed directly to the correct personnel only.
3. All email communication must be with employees of Hodge Hill College or authorised companies such as Local Authority or other Schools. Under no circumstances must you subscribe to any service, which has not been approved.
4. If you receive any harmful content from internal/external recipient, please report it immediately to the Business Manager or the ICT Operations Manager.
5. Hodge Hill College reserves the right to review, audit, intercept, access and disclose all messages created, received or sent using the email system.
6. All email accounts are maintained by Hodge Hill College. Under no circumstances must account credentials be given to other staff members. All email account passwords must comply with the following rule – Minimum of 8 character, upper-case and lower-case characters and at least one number.
7. Staff should never use another persons' email account also never disguise or attempt identity when sending emails.
8. Staff should check their emails on a regular basis throughout the day and action email messages within a reasonable timeframe.
9. Do not allow anyone else to use your email ID and password, or leave your email logged on and unattended so that others could interfere with it. You will be held responsible for any inappropriate email activity using your accounts. Staff have full responsibility to manage their email account and to ensure that they meet and adhere to the guidelines and policies. Emails need to be deleted in accordance to their sensitivity and message content.
10. Any emails that are deleted can be restored from the Office 365 platform, currently it is 30 days from the date of deletion.
11. Under the Freedom of Information Act 2000 and Data Protection regulations 1998, school emails can be disclosed and therefore be made public. Please remember, if you delete an email, the recipient(s) may still have a copy of the email, which can also be disclosed. An email remains within the system up to a maximum of 30 days after deletion is made.
12. An email agreement could potentially be formed into a contract. Under no circumstances must staff enter into any agreements with internal staff or external agencies unless prior arrangements have been approved.
13. There is a risk that incoming emails could interrupt Teaching and Learning. To mitigate this risk please turn off unnecessary notifications such as read/delivery reports.

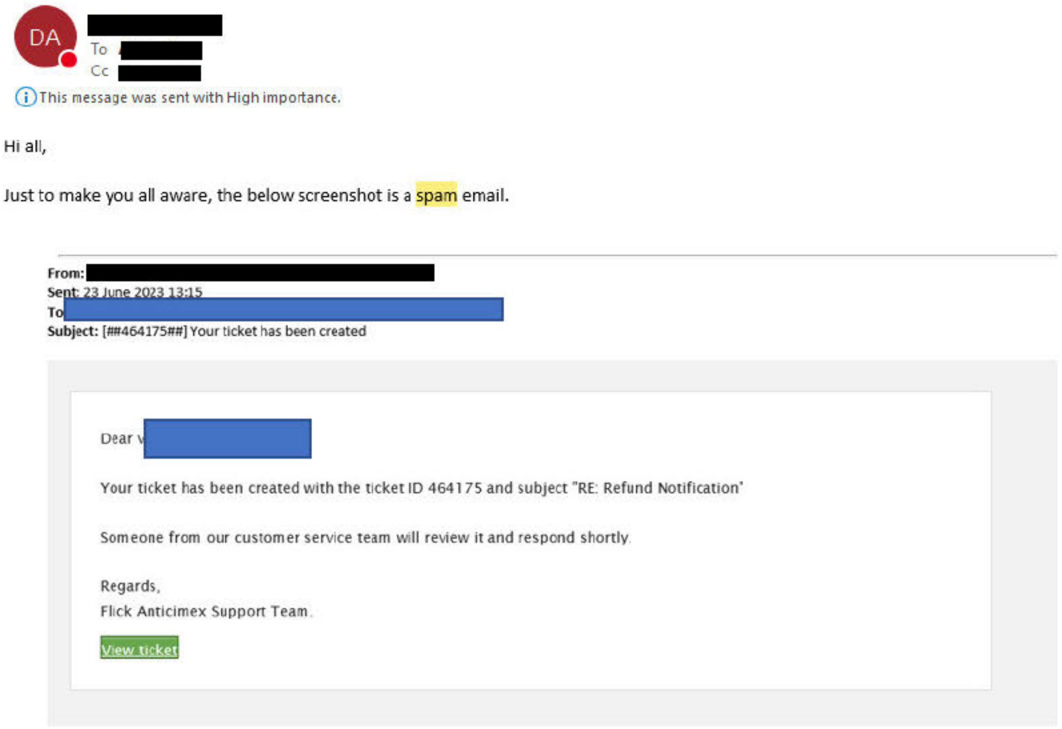
14. The Out of Office message will need to be configured on your email account for the period of a scheduled absence. This will notify the sender to contact other colleagues if required. A typical 'Out Of Office' response is below.

Hi

I am currently out of the office, returning on 13th October 2018. In case of any emergency, please contact the Supportdesk and one of the team will be able assist accordingly.

Thanks

15. Emails need to be retained for content purposes only e.g. Is the email content referencing Pupil/Staff information. The retention period of these emails will correspond to the schedule of the Records Management Tool Kit for Schools.



[redacted]
To [redacted]
Cc [redacted]

This message was sent with High importance.

Hi all,

Just to make you all aware, the below screenshot is a spam email.

From: [redacted]
Sent: 23 June 2023 13:15
To [redacted]
Subject: [##464175##] Your ticket has been created

Dear [redacted]

Your ticket has been created with the ticket ID 464175 and subject "RE: Refund Notification'

Someone from our customer service team will review it and respond shortly.

Regards,
Flick Anticimex Support Team.

View ticket

15th September 2020

Acceptable Use Policy Addition Remote

Learning

1. Remote learning will only take place using Class Charts and Google Classrooms (for Computer Science)

2. Staff will only use school managed 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/setting laptop, tablet or other mobile device. Where this is not possible staff should access the school network via a VPN or through Foldr.

- Use of Google Classrooms for teacher feedback is only approved when working from the school network.

3. Pupils have been given accounts generated by the school to allow access to resources, submission of work and teacher feedback.

- On Google Classrooms email is disabled and the accounts are to be set up to ensure the user names cannot be used to log onto any services that google provide (such as YouTube), that the school as deemed inappropriate for general use.

- Collaboration between pupils is to be disabled with pupils' access rights set so they cannot post messages on the open message boards or to allow private chats between peers to ensure that the platform cannot be used for inappropriate messaging or behaviors.

- Any app that the G-Suite accounts assigned to pupils can assess that can be used for general student to student communications are disabled by default on all school accounts.

4. Live streamed remote learning sessions are not permitted.

- If there is a need for recorded lessons, then agreement from the head teacher must be obtained prior to production and personal equipment must not be used.

5. Any resources uploaded should be from the subject area on the school network.

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

6. Access to Class Charts and Google Classrooms will be managed in line with current IT security expectations.

7. Teachers must report any behaviour or safeguarding concerns using the school systems

on Class Charts in line with our safeguarding and child protection policy.

- Pupils should not be submitting images of themselves. This needs to be referred to the AC for the year group.

8. Teachers should treat any communication with pupils as professional conversations as they would have in everyday interactions with pupils.

- Class Charts hold a record of all information sent between pupils and teachers and all work shared with pupils can be viewed by Admin account holders (DOLs and SLT).

- For each class on Google Classroom a second member of staff should be allocated so all work and communication can be monitored. Classes will also have a member of SLT attached for further monitoring and safeguarding.