IBAT College Dublin

ICT Security Policy

Version 1.8 August
2023

Contents

Purpose

The purpose of this IT security policy is to protect the information assets of the IBAT College Dublin from all threats, internal, external, deliberate or accidental. The policy is aimed at:

- Safeguarding the availability, confidentiality and integrity of the College's information.
- Protecting the IT assets and services of the College against unauthorised access, intrusion, disruption or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.

The policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

Policy Scope

The IT Security Policy covers procedures and standards relating to:

- IBAT College Information Assets
- IBAT College ICT Resources

The IT Security Policy applies to all stakeholders who use IBAT's IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices. The IT Security Policy also takes precedence over any policies which may be developed at a local level.

Roles and Responsibilities

IT Services are responsible for monitoring use of IBAT's ICT Resources in-line with this Security Policy.

IT Services and the Data Protection Officer (DPO) are responsible for enforcing effective operation of the Information Security Policy to ensure that information assets and technologies are adequately protected.

All stakeholders are required to demonstrate compliance to IBAT's Security Policy in order to protect the confidentiality, integrity, and availability of IBAT's Information Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to IBAT.

Confidentiality

Safeguarding the confidentiality of information through the protection of information from unauthorised disclosure with access only by entitlement.

Remote Working

With IBAT working from home is critically important to be aware of the risks around cyber-attacks from home, particularly ransomware. To combat this growing threat, we must all take the time to become educated on these threats and ensure we don't become victims.

What is Ransomware?

Ransomware is commonly spread via fraudulent emails, either as an infected email attachment containing malware or downloaded directly from the scammer's website. IBAT College has anti-virus scanning systems in place for detecting viruses on its network and Google is very good at filtering most of these emails, but with the current targeting of Irish HE Institutions we must all still be vigilant and exercise additional caution particularly with using company or personal computers at home for remote working.

It's also very important to realise that Ransomware is brutal and indiscriminate, it doesn't care if it infects an IBAT or personal computer, the result is the same, it will infect all documents, photos, videos and other important files so they are encrypted and cannot be opened or you're completely locked out of your computer; you are then held to ransom and asked to pay (usually bitcoin) to unlock your computer and/or unencrypted your files.

We have included these questions regarding ransomware and phishing which can help protect you against these types of cyber-attacks.

What is phishing?

Phishing is a form of online fraud. Scammers use phishing emails to trick you into giving away important information, such as your login details. They can then use these details to access your own data and login to IT systems, putting your own computer and potentially the College at risk

In a typical phishing incident, you may receive an email or pop-up message that claims to be from IBAT or another business or organisation that you may have previously dealt with for example eBay, PayPal, Revenue or Bank of Ireland. The message may ask you to 'update,' 'validate,' or 'confirm' your account information.

How can I identify a phishing email?

It is easy to be alarmed by a phishing email, they are designed to get us to act without question. They may appear to come from a legitimate business that you have previously dealt with or a colleague. Always trust your instincts, stay cautious, always take your time and consider the validity of the email, if an email offers something that looks too good to be true, it possibly is. Similarly, don't be tempted to respond hastily to an email which threatens to disable your account.

Phishing emails often have the following types of characteristics:

- They may use language like 'important notice', 'urgent update' or 'alert' or 'violation' with a deceptive subject line to persuade you that the email has come from a trusted source.

- They may contain messages that use threatening language, stating that your account will be disabled if you do not act.
- They may appear to come from someone in IBAT, but you should be aware that email addresses can be forged easily.
- They may copy content such as logos and images used on legitimate websites to make the email look genuine.
- They may contain hyperlinks that will redirect you to a fraudulent website instead of the genuine links that are displayed. If you see a link in a suspicious email message, don't click on it, if you are unsure, please contact IBAT IT Support at: it.support@ibat.ie
- All legitimate IBAT website addresses will always include ibat.ie as the main domain and will never include ".com", valid examples are shown below, these would typically be at the start of a legitimate IBAT web address:

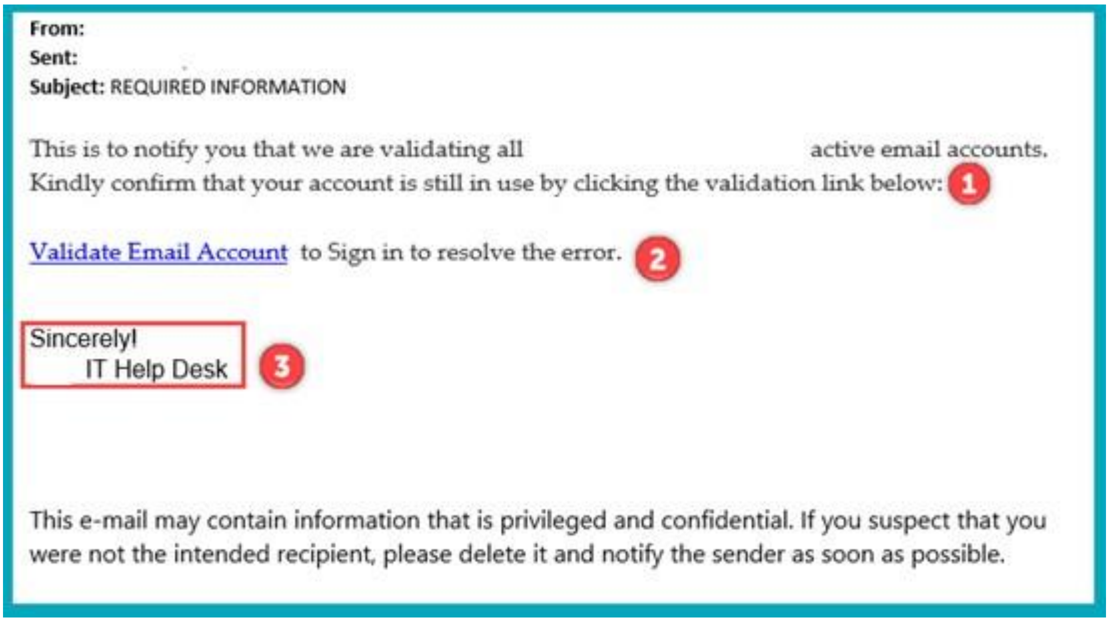
Look at the example of a phishing email message sent to students and staff below, this would be a typical example of the type of phishing email been sent to staff and students.

- https://www.ibat.ie/
- https://www.ibat.ie/payments/
- http://intranet.ibat.ie/
- https://my.ibat.ie/helpdesk/
- https://my.ibat.ie/moodle/
- https://services.ibat.ie/ https://mail.google.com

And any legitimate web addresses from Google will always include "google.com"

- https://classroom.google.com
- https://drive.google.com
- https://meet.google.com
- https://support.google.com/

- If sent from IBAT, the sender email will always include a valid @ibat.ie address and will most likely be already known to you, or it will include a valid @ibat.ie email group such as: it.support@ibat.ie, studentsupport@ibat.ie, online.support@ibat.ie.
- IBAT will never ask you to verify any of your information over email or SMS, we can always do this face-to-face using Google Meet or MS Teams if necessary.
- If you are asked to go to an external link, you can check where this link will bring you by hovering over the link name.
  You can then see the address and confirm if the start of the URL matches the valid "ibat.ie" addresses shown above.
- Watch for unusual sign-off, we would never include "Sincerely!!" or "Help Desk"



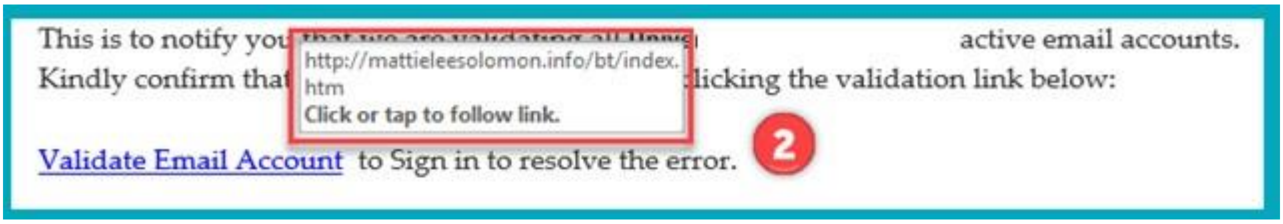
From:
Sent:
Subject: REQUIRED INFORMATION

This is to notify you that we are validating all active email accounts. Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account to Sign in to resolve the error.

Sincerely!
IT Help Desk

This e-mail may contain information that is privileged and confidential. If you suspect that you were not the intended recipient, please delete it and notify the sender as soon as possible.



This is to notify you active email accounts.
Kindly confirm that licking the validation link below:

http://mattieleesolomon.info/bt/index.htm
Click or tap to follow link.

Validate Email Account to Sign in to resolve the error.

Please spend 2 minutes viewing the YouTube Video below: https://youtu.be/YfiN_W8I1cE

What is ransomware?

Ransomware is a type of malware, where scammers aim to trick their targets into downloading malicious software on their computers in order to encrypt their files or lock them out of their devices. If you fall victim, the scammer demands you to pay a ransom in order to recover your files and/or regain access to your device.

Please spend 5 minutes viewing the YouTube Videos below:
https://youtu.be/Vkjekr6jacg https://youtu.be/kAfO4Rg2In4

What should I do if I receive a phishing email?

Please report any email that you believe is phishing to the IBAT IT Support (it.support@ibat.ie) as it may have also been sent to other IBAT staff members.
Remember treat any email that asks for your username and password with extreme caution.

What should I do if I have fallen for a phishing scam?

If you think you have fallen prey to a phishing email, immediately report the incident to the IBAT IT Support: it.support@ibat.ie

Change your password immediately, below is a link with the steps needed to change and/or reset your password. https://support.google.com/accounts/answer/41078?co=GENIE.Platform%3DDesktop&hl=en

I'm also including the link below again which outlines the importance of protecting your @ibat.ie Google account and the action needed to add 2 step authentication, if this still needs to be done, then please follow the instructions provided. https://www.google.com/landing/2step/

Backup your Data

Backup your data, files and devices regularly – this will help you recover any lost or damaged data/files should you fall victim to ransomware.

It's important to note that the responsibility for backing up data held on personal devices needs to done by staff member as we cannot backup personal devices or those outside the IBAT network. Please ensure all company files are stored in the designated company drives and folders (Z: Datafile and S: Shared) on the IBAT Network.

Please note that all IBAT staff have their own personal network drive/folder (H: Drive), any files that cannot be stored into the shared company drives/folders above should be store in the personal drive/folders provided so they are included with the daily backups.

All staff also have an @ibat.ie Google account which includes Google Drive, many staff have been using Google Drive extensively for sharing files, it can also be used as a secondary backup, so in the event that your computer is compromised and files become infected you still have these files safely stored in the cloud with Google Drive and separate from your computer.

Be Vigilant

Do not download or open files from unsolicited emails. If you receive an email with attachments you were not expecting from someone you know, check with that sender before acting on the email.

If it's been sent your @ibat.ie email then please report it to IBAT IT Support (it.support@ibat.ie) as it may have also been sent to other IBAT staff members.

Some more top tips to protect your privacy.

- **Keep work and social life separate.** Only use your IBAT email address and accounts for work related purposes. Use a personal email address for social and domesitic websites and apps.
- **Use unique, long and complex passwords or passphrases**. IBAT passwords must be unique. The length and complexity of your passwords can provide an extra level of protection for your personal information.
- **Take care what you share.** Periodically check the privacy settings for your social networking apps to ensure that they are set to share only what you want, with whom you intend. Be very careful about putting personal information online. What goes on the Internet usually stays on the Internet.
- **Go stealth when browsing**. Your browser can store quite a bit of information about your online activities, including cookies, cached pages, and history. To ensure the privacy of personal information online, limit access by going "incognito" and using the browser's private mode.
- **Using Wi-Fi?** If only public Wi-Fi is available, restrict your activity to simple searches (no banking!) or use a VPN (virtual private network). The latter provides an encrypted tunnel between you and the sites you visit.
- **Should you trust that app?** Only use apps from reputable sources. Check out reviews from users or other trusted sources before downloading anything that is unfamiliar.
- **Know your rights.** Become aware of your data protection rights and the responsibilities of those who hold and process your personal details. You can find more information here.

Personal Information is like money, Value it, Protect IT

Think before you act: Be wary of communication that implore you to act immediately, offers something that sounds too good to be true or ask for personal information.

Guard your date of birth and telephone number: These are key pieces of information used for verification, and you should not share them publicly. If an online service or site asks you to share this critical information, consider whether it is important enough to warrant it.

Get two steps ahead: Switch on two-step verification or multi-factor authentication wherever offered to prevent unauthorised access.

Secure your devices: Use strong passwords or passcodes or touch ID features to lock your devices. Securing your device can help protect your information if your device is lost or stolen and keep prying eyes out.

Think before you app: Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value? just like money. Be thoughtful about who gets that information and how it's collected through apps.

Get savvy about WiFi hotspots: Public wireless networks and hotspots are not secure – this means the possibility exists that anyone can see what you are doing on your laptop or smartphone while you are connected to it. Think about what you are doing and if you would want another person to see it. If you use public WiFi , think about using a virtual private network (VPN) that provides a more secure WiFi connection.

Now you see me, now you don't: Some stores and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi and Bluetooth when not in use.

Share with Care

What you post can last a lifetime: Before posting online, think about how it might be perceived now and in the future and who might see it. Share the best of yourself online.

Own your online presence: Set the privacy and security settings on web services and devices to your comfort levels of information sharing. It's ok to limit how and with whom you share information.
Click here for more information.

Be aware of what's being shared: Be aware that when you share a post, picture or video online, you may also be revealing information about others. Be thoughtful when and how you share information about others.

Post only about others as you have them post about you. The golden rule applies online as well.

Email Policy

The purpose of this Policy is to set out the conditions under which the College's email system – Google Mail – may be used, and the principles for managing messages created or received as part of the College's business. It applies to all staff and other authorised account holders.

Electronic Mail is a tool provided by IBAT College Dublin and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of College email accounts evidences the user's agreement to be bound by this policy.

Ownership

All @ibat.ie email addresses, associated accounts, work-related emails and instant messages are the property of the College. Ownership allows the College the right to access/monitor emails and, if necessary, their content.

Personal data

Google Mail and its related applications (e.g. Google Drive, Google Calendar, Google Meet) are hosted in the cloud. Google handles all personal data in line with its Privacy Policy (www.google.co.uk/policies/privacy/) and adheres to the European Union Privacy Shield (www.privacyshield.gov/EU-US-framework). The College is signed up to the JANET contract with Google, which addresses the requirements of Irish Data Protection legislation.

Legislation

Please see the Appendix for a brief description of the main pieces of legislation that have a bearing on the use and transmission of emails.

Conditions of use

Email facilities are provided to support learning, teaching, research, administration and approved business activities of the College. Refer to page 8 regarding personal use conditions.

Account Creation

Name used to create e-mail account:

IBAT College email accounts are created based on the official name of the staff or faculty member as reflected in Student Management System and HR records. Requests for name changes to correct a discrepancy between an email account name and official College records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis by the IT Support Team: itsupport@ibat.ie.

Responsibility:

- Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.
- Staff are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding College matters sent from an administrative office, faculty, or staff member is considered to be an official notice.

Set-up considerations:

Emails and instant messages (which are saved in Google Apps, if one or more of the people involved in the conversation have the history set to "on the record") are potentially disclosable to external parties and statements must not be made that could expose the College to legal liability or damage its reputation.

Legal Framework:

Emails are subject to the same laws and policies that apply to other forms of communication, including the relevant data protection legislation and the Freedom of Information Act 2014, and must be composed using the same degree of care as would be used for a formal letter.

All communication undertaken on behalf of the College is subject to the College's Data Protection and Privacy policy (available at https://www.ibat.ie/privacy-policy.html). In addition account holders must comply with the G Suite Acceptable Use Policy (available at www.google.com/apps/intl/en/terms/use_policy.html).

Security

Users are responsible for the security of their mailboxes.

Vigilance (Viruses):

Although emails are automatically scanned for virus content and spam, account holders are expected to take reasonable measures to prevent the introduction and transmission of computer viruses. These include:

- not opening attachments received from unsolicited or untrusted sources;
- not transmitting attachments known to be infected with a virus;

Strong Password:

Users should use strong passwords and must never disclose their passwords to others. A strong password contains at least one upper case letter, number and symbol. If it is necessary to provide another user with access, delegation should be employed, which enables authorised access without the sharing of passwords.

Two-factor authentication:

In addition to a strong password, the College strongly advises the use of two-factor authentication for Google accounts (https://www.google.com/landing/2step/).

Managing SPAM:

Google Mail automatically helps identify spam and suspicious emails and will place these into your Spam folder (label). Staff can also teach Google Mail what is spam by highlighting emails in your inbox and clicking the "Report Spam" button. This will send the message to your Spam folder and remove it from your inbox, and Google Mail will continue to do the same if you receive future emails from that sender. If you make a mistake and do not want the message to be in Spam, click the "Not Spam" button to move it back into your inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message.

Lock your workstation:

All staff should lock their workstations (Ctrl+Alt+Del on Windows) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

Report:

Users may not monitor, intercept or browse the messages of others, unless authorised to do so. The IT Support Team should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to his/her account.

Prohibited use

Staff should always use their College email address to conduct College business, as Google Apps Mail is webbased and can be accessed from any location with internet access. This is to ensure that the College has a record of all business correspondence and to enable the College to back up work-related emails for business continuity purposes. In addition, provision has been made for offline access to emails, when necessary.

The College email facilities **must not be used** for:

- using or attempting to use the accounts of others without their permission;
- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing, libellous or defamatory;
- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- the creation or transmission of material that brings the College into disrepute;
- the creation or transmission of material that is illegal;
- the incitement of violence;
- unauthorised transmission to a third party of confidential material concerning the activities of the College;
- the transmission of unsolicited commercial or advertising material, chain letters or other junk mail;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- excessive or unreasonable personal use.

Other examples of improper use of the email system include:

- generating or facilitating unsolicited bulk email;
- infringing on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- violation, or encouraging the violation of, the legal rights of others or national laws;
- any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;

- intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- interfering with the use of the email services, or the equipment used to provide the email services, by students or other authorised users;
- altering, disabling, interfering with or circumventing any aspect of the email services;
- tests or reverse-engineer the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- content that:
  - (i) constitutes, fosters, or promotes pornography ;
  - (ii) is excessively violent, incites violence, threatens violence, or contains harassing content;
- creates a risk to a person's safety or health, creates a risk to public safety or health;
- compromises security, or interferes with an investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- misrepresents the identity of the sender of an email;
- using or attempting to use the accounts of others without their permission;
- collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);
- use of the service to distribute software that covertly gathers or transmits information about an individual;
- conducting business for profit under the guise of the College;
- Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of IBAT College Dublin.

This list is not exhaustive. Inappropriate use such as activities referred to above may result in the suspension of a user's email facilities for as long as necessary to conduct an investigation. The instigation of formal action under the staff disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

Personal use

Permission & Restrictions:

Modern technology makes it easy to check personal email accounts on mobile devices, anywhere, anytime. Staffs are permitted a limited level of personal use within their work email account, but should be mindful that it must not:

- be detrimental to the main purpose for which the facilities are provided;
- conflict with College objectives, values, or interests;
- conflict with the College's rules, regulations, policies and procedures;
- conflict with an employee's obligations to the College as their employer;
- involve personal financial gain or be of a commercial or profit-making nature that could take the individual away from their own work);
- involve significant use to pursue personal legal or domestic issues.

How to manage personal mails:

- Staff should ensure that either any messages addressed to or sent from their work email account for private purposes are clearly identified as personal and filed within a separate folder, or are deleted as soon as practicable. Separating personal emails from work-related information (or deleting them) will help delegated access users to avoid breaching the privacy of others when checking mail on behalf of absent members of staff.
- Staff who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.
- Staff should be aware that personal email sent from a work account may still need to be disclosed if the College receives a request under relevant information disclosure legislation (e.g. Freedom of Information and Data Protection legislation etc). Likewise, information disclosure requirements may also apply to work related emails sent from a personal email account. For this reason, personal email accounts should not be used for sending or receiving work related emails.

Distribution group emails

Group distribution list are a useful means of conveying information and, when necessary, important and urgent messages to all staff of the College. It is, however, important that the facility is used appropriately and only by designated and authorised staff.

These all-staff emails are for the timely dissemination of information considered important to all staff and may encompass the following categories:

- Important IBAT College related news or announcements
- GUS newsletter and corporate correspondence
- Academic correspondence and information relevant to each school
- Information relevant to the operation or suspension of IT systems
- Health and safety matters
- Access issues where buildings may be affected
- Governance and legal compliance matters
- Critical incidents

Use of distribution lists or ‘reply all’ features of email should only be used by authorised staff and only for legitimate purposes as per these guidelines.

Monitoring

Account activities (e.g. storage usage, number of log-ins) are monitored by Google and all messages are routinely scanned (for viruses, spam and other security threats) to assist with the effective operation of the email system. This process is completely automated, and no human intervention is involved. The use of all personal information by Google is governed by its Privacy Policy (www.google.co.uk/policies/privacy/).

The College, as the domain administrator for Google’s facilities, may have access to information held in an email account. The College reserves the right to access this information in the following circumstances:

- in connection with a criminal investigation;

- in connection with a properly authorised and evidenced investigation in relation to breaches or alleged breaches of the College's rules on use (including but not limited to whistleblowing, fraud and bribery);
- to meet legal or statutory requirements;
- in a situation (such as prolonged staff absence) where access is required to enable the College's business to continue; (Refer to page 3, point 7 about Delegate Access).
- in an emergency situation.

Where there is evidence of an offence, it will be investigated in accordance with the College's disciplinary procedures.

Confidentiality

Appropriateness & Attachments

Email, like any other form of communication, is not completely secure and its confidentiality cannot be guaranteed: messages can be intercepted by third parties, wrongly addressed, forwarded accidentally and forwarded by recipients to third parties. Before transmitting information of a confidential nature, users should assess whether it is appropriate to transmit the data in the email itself, or whether it should be in a document attached to/linked from the email. If documents containing sensitive information are sent from the College's network to external addresses, then staff must password protected and encrypt the attachments first.

For guidance on how to encrypt documents please review these websites links:
https://www.groovypost.com/howto/geek-stuff/password-protect-encrypt-microsoft-office-2010documents/

https://www.groovypost.com/howto/password-protect-encrypt-office-2016-documents-excel-wordpowerpoint-o365/

Forwarding:

Before forwarding messages, whether externally or internally, staff should consider whether the authors of the messages would expect or be willing for this to happen. Staff should also consider whether the transmission of the information would breach the privacy of an individual or infringe copyright. In cases where it is necessary to send a message to a number of individuals – some (or all) of whom do not work for the College – care must be taken to prevent the recipients' email addresses from being disclosed **Transparency:**

The **'BCC' facility** should be used to ensure that the addresses of the recipients cannot be viewed by each member of a distribution list.

Monitoring and record keeping:

Work-related emails are records of the College's actions and decisions, and must be managed as efficiently, and in the same way, as paper and other electronic records. There should be consistent, coherent controls in place to meet business and accountability needs, as well as to ensure legal compliance.

Messages must be checked regularly, prioritised and answered as promptly as possible. They should also be stored logically to ensure that information can be managed effectively and readily retrieved in response to enquiries (such as Data Protection and Freedom of Information requests).

Staff is encouraged to tag emails with Labels, Stars and importance tags to aid the management of current mail and retrieval of archived mail.

Access by Google:

Google also retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy

http://www.google.com/a/help/intl/en/admins/use_policy.html

Training and Guidance

Online training on the use of Google Mail and other G Suite applications are available at:

https://gsuite.google.com/training/

Email Signatures

In order to present a consistent and professional image to those with whom the College corresponds, staff is expected to adhere to corporate guidelines when creating their email signature.

The logo used in the signature will be reviewed regularly and, where appropriate, updated to reflect those that most enhance our reputation. Staff will be informed when the logos to be used in the approved email signature change.

The format is as follows;

- Sign off
- Name | Role
- IBAT Logo
- Campus Address
- Contact details – Campus Main Switch, Direct Dial (if applicable), e-mail, website.

For example

Kind regards

John Doe | **Lecturer**

ibat COLLEGE DUBLIN

16-19 Wellington Quay, Temple Bar, Dublin 2, Ireland

T +353 1 807 5055 **DD** +353 1 246 1508 **E** **john.doe@ibat.ie** **W** www.ibat.ie

Retention & Deletion

For further information please refer to Associated Policies 1.9, College Data Protection and Record Management Policy and 1.10 Data Retention Schedule that accompany the College Quality Assurance Handbook, 2021 V4.5

It is the responsibility of all staff to ensure that messages with continuing value are saved. Emails cannot be treated as a single series with a single retention period: the length of their retention must be determined by their subject matter or business purpose, as is the case with any other electronic or paper record.

Retention decisions should take into account business/operational needs, legal and regulatory requirements, accountability and transparency expectations. Messages relating to complaints, appeals, disputes and grievances should be retained as long as there is a need to preserve an audit trail.

The risk implications of deleting messages must be considered, as well as the obligation to comply with Data Protection legislation.

Google offers unlimited email storage, but this must not be abused. Staff is obliged to review their emails (both their inbox and their archived mail) on a regular basis to ensure that those that have served their purpose are deleted. Messages that are no longer needed should be moved to the Bin. Staff should be aware that all items placed in the Bin will be automatically deleted after thirty days and cannot be recovered. Whilst information is held in the Bin, it will be considered still accessible and may therefore have to be disclosed (in the period before erasure) in response to requests made under Freedom of Information or Data Protection legislation.

Shared email accounts

In departments where several staff are responsible for work activity and require access to the same emails, sharing access to a single account can make it easier to answer messages promptly and manage them effectively when individual members of the team are away.

Using a shared email delegated account should also simplify the process of sorting accounts when staff leaves: if team members keep the majority of their emails in a shared mailbox, less time should be required for reviewing individual accounts when staff leave the College.

Each shared delegated email account requires a primary contact that is responsible for the overall management of the mailbox, ensuring there are effective procedures in place for controlling incoming and outgoing messages.

Staff or departments can request temporary delegated shared access to email accounts. Staff requesting these types of account will be required to submit user information, rationale for account and expiration date to their Line Manager or Head of School (HoS)for approval. Following approval, a request can be logged with the IT Support Team: itsupport@ibat.ie

Staff should be aware that when they allow a colleague delegated shared access within Google Mail, they are granting full read and write access to that person. However, any emails sent from an email address using delegated permissions will need to be clearly identified as to the real author for each recipient.

Unless otherwise agreed between the user and their delegated colleague, access should only be used in times of absence or emergency. Anyone who is granted access to another user’s account must respect the confidentiality of that account and must not view data that is clearly of a personal nature.

Absence from the College

In cases of planned absence, staff must set up an out-of-office message giving alternative contact details to ensure that enquiries can be answered promptly.

Illness or other unforeseen circumstances

In cases of illness or other unforeseen circumstances, where it is not possible to make any preparations for being away from the office, delegate access to your account will be through your line manager or the IT manager and not accessed by your peers.

The following actions are required by line management or HoS in the case of academic staff:

- Set up an automatic reply. To do this, the line manager or HoS should log a request with the IT Support Team, requesting that an auto-reply is added to the relevant staff account and supplying the exact text for the reply.
- Set up an auto-forwarding facility, if necessary. To request auto-forwarding, the line manager or HoS should similarly log a request with the IT Support Team: itsupport@ibat.ie
- Ensure emails received in the intervening period are dealt with, as necessary. If the line manager or HoS needs to gain access to the account to check whether there are business emails requiring attention, they should log a request with the IT Support Team: itsupport@ibat.ie

Leaving a department or the College

When members of staff leave the College, it is their responsibility to delete all personal messages and, in some instances, transfer access to appropriate colleagues.

Staff should be aware that, once they have left the College, they will no longer have access to their @ibat.ie email account, as this is the property of the College. It is therefore important that they remove all their personal emails – any items of a personal nature that they wish to retain should be forwarded to a private email address in advance of their departure.

It is also the responsibility of each staff member to ensure that an appropriate out-of-office response is set up to inform senders that they have left the organisation and give them alternative options for submitting their enquiry to another email address or department.

Expiration of Accounts

Staff and students may leave the College for a variety of reasons, which has implications on the duration of email privileges or when an account expires. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, the College reserves the right to revoke email privileges at any time.

- Staff members who leave the College will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.
- Staff who have retired from the College will have email privileges removed effective on their last worked day.
- Students who leave the College without completion of their studies may keep their email privileges for one academic year from the last term when they were registered.
- Expelled students - If a student is expelled from the College, email privileges will be terminated immediately upon the directive of the Registrar’s Office.
- Students who have graduated from the College will be permitted to retain their email account for a period of one year, follow which their account will be terminated.

Local File Backup Policy

Background

Local Data Files are files that are IBAT College related information and mission critical data that are saved on your **Local Hard drive**.

What is a Local Hard Drive? A physical hard disk that is in your own PC where you save all the information on a specific folder such as “My Documents”

What is H Drive or Home Folder? This is a folder located on the network and not in your local hard drive. Home folder or Personal folder is part of the Z Drive Data File \ Users folder where you can save Corporate Data from your local hard drive to your own Home Folder.

Home folder is only accessible to the folder owner and cannot in any way be accessed by other staff.

A disaster can happen anytime such as Physical Error, Virus Infection, Natural or Environmental that will cause all your files to become accessible or possibly be deleted and become unrecoverable and unusable. Each staff has been provided with a Personal Folder on the network without limitation to be able to copy, backup or synchronize their data to and from.

Losing your data is disastrous, so regular backup is a must so that if disaster occurs, the IT Department are able to restore your data based on your latest backup.

Objective

- To ensure business continuity for all staff when disaster occurs.
- To provide information for all staff of the importance of regular back up.
- To be able to Backup and Restore Local Data Files when disaster strikes on staff Local PC or Laptop.
- To provide awareness for staff in terms of Data Protection and Security.

Policy

All Local Data Files that are ONLY related to company should be saved or backup to H Drive or HOME FOLDER on the File Server.

It is generally recommended that you store your most Corporate Data in your H Drive or Home Folder in the network.

Staff and Lecturers are given a personal storage on the network which should be used for storing and backing up company related files.

A simple copy and paste procedure is the only process for now to copy or back up your files from the “My Documents” folder to your H Drive or Home Folder.

Simple Copy and Paste Procedure

1. Make sure the file is **Closed**.
2. **Right click** the file on your local drive.
3. Choose **Copy** (nothing will happen after this.)
4. **Go** to your **H Drive or Home Folder** and choose a folder where to copy the file.
5. **Right click** the correct folder destination and choose **Paste.** Please see policy no. D11 for Overwriting Files.
6. You can also copy a whole folder but be careful on the overwriting process.

User Responsibility

It is the responsibility of all staff to keep his or her Local Files to be backed up regularly in the H Drive or Home Folder.

- It is the responsibility of all staff to back up ONLY company related data and not personal data.
- It is the responsibility of all staff to protect and secure their Local Data File stored on their Local Hard Drive
- IT Department DO NOT recommends backing up Corporate Data in an external storage or USB stick without permission from the IT Department for security reasons.

IT Department and Exceptions

- Special software will audit file access and back up time for each staff in order to monitor the time and date of your last backup so that we can restore whatever latest information based on the audit and in your last backup.
- IT Department is responsible for backing up all Corporate Data saved on the Z Drive including staff Home Folder.
- IT Department is responsible for keeping the Corporate Data secure and should be backed up regularly in accordance to the Network Backup Policy.
- IT Department will NOT be held liable for any loss, deleted, corrupted data on your local drive if this policy has not been followed accordingly.
- IT Department is NOT responsible for accidental OVERWRITING with your existing files on the H Drive or Home Folder. Please ensure that before deciding whether you will overwrite the file/s & folder/s or not, please review the changes first and the target document itself.
- Windows Systems detects if the file you are copying already exists on the destination. A confirmation will pop up on the screen that will compare the file that you are copying and the file already there, and this gives you the decision if you want to overwrite it or not.
- Windows will give you detailed comparison of the file size, date and time of modification etc. So you must be aware of these details. Overwritten files are irreversible.

- IT Department treats every single document as highly classified information and should not be opened and read, sent out by email or distributed without proper authorization from senior management.
- IBAT College Dublin reserves the right to review and or require change of any identification and/or authentication process for compliance with this policy.