St Edmund's College & Prep School

STAFF ICT ACCEPTABLE USE POLICY

Rooted in Christ and Catholic tradition and under the guidance of its patron, St Edmund's aims to realise the God-given potential, in body, mind and spirit, of all members of its community through service and leadership.

Avita Pro Fide

St Edmund's is committed to ensuring the welfare and protection of children in its care and this commitment is a fundamental part of the role of every person employed by St Edmund's.

Introduction

St Edmund's College embraces the use of IT to enhance teaching and learning and the College's administrative processes. This policy covers the acceptable use of IT, data and communication systems and applies to all members of St Edmund's College staff including teaching and non-teaching staff, Governors, and volunteers.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the College's IT systems and infrastructure.
- Define and identify unacceptable use of the College's IT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the IT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

And to ensure that:

- The integrity of the information is maintained.
- Confidentiality is always maintained.
- Information is readily available to the relevant users throughout the College.
- Staff understand their responsibilities when using IT facilities to ensure the welfare and safeguarding of students.
- Data access and use conforms to regulations in regard to the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.
- Undesirable consequences associated with breaches of information security are avoided. This includes but is not limited to bad publicity, fraud and the illegal use of personal data.
- Staff understand the boundaries of acceptable behaviour and to mitigate the risk of inappropriate communication taking place between staff and students.

This policy applies when accessing:

- College data and information stored in an electronic format which relates to the wider community;

- The College computer network (e.g. shared drives), information systems (e.g. iSAMS) and online collaboration systems (e.g. Microsoft/Office 365). This is by any means or device, whether directly or remotely on either College or personal devices;
- The internet, social media or other online communications platforms whether through the College network or through personal devices during the hours of employment, conducting school business and/or representing the College.

This policy should be read in conjunction with other policies within the Staff Handbook including but not limited to:

- Data Protection Policy
- School Privacy Notices
- Information Security Policy
- Taking, Storing and Using Photos of Children Policy
- Code of Conduct for Staff Policy
- Safeguarding CP Policy

All users of the College's IT systems are expected to read and understand this policy.

All official College business must be conducted using College systems (including online services such as Microsoft/Office 365). Student/Staff personal data must not be stored on non-College systems including USB memory sticks.

The use by staff and monitoring by the College of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the College's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Bursar, the Deputy Headmaster (Pastoral) or the Technical Projects Director.

Provision of IT Systems

All equipment that constitutes the College's IT systems is the sole property of St Edmund's College. Users must not try to install any software on the IT systems without permission from the IT Department.

The IT Department is responsible for purchasing and/or allocating IT equipment to individuals. Individual laptop/desktop computers or IT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

IT equipment that is allocated to individuals must be treated with care and kept secure in locked offices, locked cupboards and, if taken home, not left in personal vehicles while unattended and must be secured in your home overnight. Users could be held personally liable for any costs incurred in rectifying any damage to IT equipment or for its loss.

Users are not permitted to make any physical alteration, either internally or externally, to the College's computer and network hardware.

Users are also not permitted to delete, destroy or modify any of the College's existing systems, programs, information or data which could have the effect of harming or exposing tor risk of harm the College, its staff, students, or any other party.

Use of Personal Devices in School

Staff may use their own personal devices (laptops, tablets, or smartphones) while in the College on the understanding that the security of the devices is their own responsibility and the College accepts no liability if the device is lost, damaged or stolen. These devices can be connected to the College's SEC_BYOD wireless network in order to access the internet and school systems but should not be used to store student and staff personal data.

Personal devices should be password protected and have up to date security software and system updates.

USB drives and external hard drives must not be used.

Network Access and Security

All users of the IT systems at the College will be issued with a network user account, password and an e-mail address. All passwords should be complex to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff members are responsible for ensuring their password remains confidential and their account is secure.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person (including family members), except to members of the IT Department for the purposes of system support.

The security of College IT systems is the responsibility of all staff who must report any security breach or suspected breach of their network, email or application account credentials to a member of SLT immediately including during weekends and school holiday periods. This includes the loss of equipment containing data, unauthorised access to a College system, the accidental transmission of College data to a third party in error or the loss of any College data in some other way. By law this may need reporting to the Information Commissioner's office (ICO) which must take place within 72 hours and swift action must be taken to notify the relevant parties in the event that their data may have been breached.

Users must not attempt to circumvent the College's IT security controls/filtering systems nor attempt to access data they are not authorised to access. This includes the use of VPN's.

Staff must be mindful of online scams which seek to obtain their username and password. If you are asked for this information, please contact a member of the IT department straight away.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the College's IT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the College's IT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

Safeguarding and Conduct with Students

Staff should understand their responsibilities with regard to safeguarding and understand that these also apply when using IT systems and equipment. Staff should refer to the safeguarding CP policy for further guidance.

College Email

College email accounts are to be used only for College business. The College's email system can be accessed from both the school computers, and via the internet from any computer.

The sending of emails is subject to the following rules/protocols:

- Language must not include swear words or be offensive, discriminatory or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the College does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official College business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email, with file level password protection whereby the password is via a different medium or by using a secure upload portal
- Access to College email systems will always take place in accordance with data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Staff must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff should respond to emails in a timely manner however there should not be the expectation of an instant response especially outside of working hours. Staff are encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts or to sign up to websites of a personal nature including online shopping websites.
- Where possible emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner. Assume that everything that you write in an email could be seen by others or by the subject of an email in the event of a subject access request or be forwarded on to other users. Always maintain a professional tone.

- All members of staff should remember that emails can be the subject of legal action for example, in claims for breach of contract, confidentiality, defamation, discrimination or harassment. This can give rise to personal liability of staff and to liability of the College.
- Think carefully before "replying to all" and ensure that you want all the recipients to receive the message.
- Review the email chain carefully before you forward an email to ensure that there isn't information further down that you shouldn't be sharing more widely.
- If emailing groups of external users, you must use the BCC field to prevent giving personal email addresses to the others.
- Copying others into an email is a legitimate way of ensuring that the necessary people are kept informed, but staff should not unnecessarily copy in others, especially line managers or members of SLT to add weight to a request. Recipients of CC emails are not required to respond and if a response is required the "*To:*" option should be used
- Never write an email if you feel angry. Allow time to consider the content before replying in these circumstances.
- Avoid prolonged email exchanges wherever possible. Email should not be used to replace a face-to-face or virtual meeting.
- Emails are a communication tool and email accounts should not be used for storing important information relating to staff, students or parents. By default, email folders have an automatic deletion feature as outlined in the College's data retention policy.

Internet Access

Staff are expected to use College IT systems responsibly and primarily for the purposes of their job role. It is understood that staff may occasionally need to use the Internet and these systems for personal use, but such use should be kept to a minimum so as not to interfere with work and responsibilities. This access should take place during break times or outside of working hours. Staff should be mindful that information or messages sent through College facilities may be attributed to the College. Personal views should be stated as such.

The College's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in the College. In this case the website must be reported immediately to the IT Department. Staff must not therefore access from the College's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral. Staff should refrain from attempting to access the dark web.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;

- sending, receiving, downloading displaying or disseminating material, which is discriminatory, offensive, derogatory, or may cause offence and embarrassment or harass others;
- sending, receiving, downloading, displaying or dissemination material which promotes violence, terrorism, religious extremism, radicalisation or that undermines fundamental British values.
- transmitting confidential information about the College and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the College);
- downloading or disseminating material in breach of copyright;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the College may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital Cameras

The use of digital cameras and video equipment, including the use of mobile phones and tablets is permitted, however staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in the College only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras for taking photos of pupils is not permitted, including those which are integrated into mobile phones, tablets or similar.
- All photos should be downloaded to the College network as soon as possible.
- Permission is required from students and/or parents and therefore staff should always assume that images and videos of students should not be shared publicly without prior permission.

Please refer to the Taking, Storing and Using Photos of Children policy for further guidance.

File Storage

Staff members have their own personal work area (OneDrive), as well as access to shared drives (including Microsoft Teams). Any school related work should be stored on one of these locations. Personal files, including personal documents, photos or music, are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.

If information/data has to be transferred it must be sent using either an encrypted or password protected method and this must be approved by the Bursar before taking place.

No school data is to be stored on a home computer, USB drive or external hard drive.

No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in the College, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips and all phone contact with parents regarding school issues must be through the College trip phones. Personal mobile numbers should not be given to students or parents.

Social Networking

Please bear in mind that even when using social media and public forums that you may still be seen as representing the College. Staff should adhere to the following when using social networking platforms:

- Staff members have a responsibility to protect the reputation of the College, staff and students always and that they treat colleagues, students and associates of the school with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the College's reputation, nor the reputation of individuals within the school are compromised by inappropriate postings.
- Members of staff will notify their line manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the College.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the College who are not directly related to the person posting them, should be uploaded to any site other than the school's website.
- No comments, images or other material may be posted anywhere, by any method that may bring the College or, the profession into disrepute.
- Staff should not accept friend or follow requests made by students on their social media accounts.
- Staff should ensure their personal social media accounts are set to private.

Monitoring of the ICT Systems

The College may exercise its right to monitor the use of its IT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the College's IT system has, or may be taking place, or the system has, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Email and Internet monitoring software is installed to ensure that there are no pastoral or behaviour concerns or issues of a safeguarding/prevent nature and this is monitored by the IT Department.

In an emergency a staff member's line manager or a member of SLT may be given access to a staff member's OneDrive and/or email account such as when a staff member is away from the College or off sick.

Other reasons for monitoring the IT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with the Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the College's IT systems, cloud-based IT systems, the internet, e-mail and/or social networking site accounts, which the Headmaster considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The College reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Author/owner of policy:	Technical Projects Director		
Reviewed by:	Technical Services Manager	Technical Projects Director	
Frequency of review:	Every 2 Years		
Policy last reviewed:	Trinity	2025	
Next review date:	Trinity	2027	
Sub-Committee approved at:	Finance Sub-Committee		