



## Acceptable Use Policy (AUP)

<b>Document Ref.</b>	<b>001</b>
<b>Version:</b>	<b>2</b>
<b>Approval Date:</b>	<b>10.10.2025</b>
<b>Review Date</b>	<b>10.10.2026</b>
<b>Document Author:</b>	<b>N Wright</b>
<b>Document Owner:</b>	<b>Trustees</b>
<b>Approved by:</b>	<b>Trustees</b>

## Table of Contents

1. Introduction .....	3
2. Scope .....	3
3. General principles .....	3
4. Key concepts .....	4
4.1 Security of assets .....	4
4.2 User IDs and passwords.....	5
4.3 Unacceptable use of systems and services .....	5
4.4 Procurement .....	6
5. Monitoring and review .....	6
Appendix One – Unacceptable use of electronic communications, systems and..... services.....	7 7
Appendix Two – Email – Principles and Guidelines .....	9
Appendix Three - Internet Use .....	13
Appendix Four – Device use – Mobile phone and tablet.....	14
Appendix Five – Device use – Scanning Documents.....	16
Appendix Six – Device Use – Personal Use of school Devices and Communication Methods .....	19
Appendix Seven - Social Media .....	21
Breaches of these guidelines .....	24

## 1. Introduction

Data, information and networks and services are vital to Brunel College. Without good use of these assets the school would be unable to provide effective and efficient teaching services to pupils and support parents. Hence an understanding of what is expected while using these assets will help individuals protect themselves and their colleagues and the school networks and services and the data processed therein and ultimately protect the school reputation.

This Acceptable Use Policy (AUP) aims to provide clarity on the behaviours expected and required by the school's staff, service providers and contractors to protect all users of data and equipment and minimise risk. It is a framework on how to conduct school business to meet legal, contractual and regulatory requirements and defines how individuals must behave to comply with this policy.

## 2. Scope

All school / trust equipment (all information systems, hardware, software and channels of communication, including voice- telephony, social media, video, email, instant messaging, internet and intranet) are within the scope of this policy. User's personal information which is processed by the school's / trust's equipment and services is also in scope.

Users are defined as all members of staff (full-time and part-time), temporary members of staff, volunteers (trustees) and contractors, and any other person or organisation acting for or on behalf of the school, that have been granted access to the school systems and data to perform a specified function / role.

All users must make themselves familiar with and comply with the guidelines at each of the appendices of this policy.

## 3. General principles

These general principles apply to user's use of school / trust equipment and services:

- Users agree to comply with this AUP and confirm that they understand that any breach of this policy may result in disciplinary action being taken.
- Users are responsible for their own actions and that they act responsibly and professionally, following the school / trust standards of behaviour and respect the school, colleagues, partners and pupils and parents.
- Users use the most efficient, effective and secure communication tools to fulfil their roles.
- All equipment and services provided by the school / trust are primarily for business use.
- Although the occasional use of equipment and services for personal reasons is permitted, its use for these reasons must not be excessive, inappropriate or interfere with carrying out any responsibilities and not adversely affect either the schoolbusiness or reputation or place the school at unnecessary risk.
- Use of information, systems and equipment is in line with the school security and information management policies.

- Do not use the school / trust equipment and services to send prohibited material that includes 'spam and unsolicited messages', 'false or misleading information', 'copyrighted material', 'illegal content or offensive material'.
- Any breach of this AUP is reported to their line manager and official procedures are followed when a breach of personal data is suspected or reported.
- Understand that they can whistle blow / raise a concern if they believe that someone is misusing school / trust assets, information or electronic equipment.
- Never undertake illegal activity, or any activity that would be harmful to school reputation or jeopardise staff and/or data that is processed on school / trust technology.
- Understand that both business and personal use of school / trust systems will be monitored as appropriate.
- Users' can have no expectation of privacy for anything that is created, stored, sent or received via the school systems.
- Should either non-compliance with this policy and guidelines or an intentional breach of this policy be discovered, senior management shall have the authority to take immediate steps as considered necessary, including disciplinary action.
- User should complete all training and awareness courses related to the use of school / trust networks and services made available to them, including data protection and cyber security courses, to make best use of equipment and services and support the understanding, recognition and reporting of threats, risks, vulnerabilities and incidents.

## 4. Key concepts

### 4.1 Security of assets

Users are responsible for the day-to-day security of school equipment and hence they must:

- Comply with the school / trust's [Physical Security Policy and Physical Security Standards] and Information Security Policy.
- Keep all portable devices that are of higher risk of theft, i.e. mobile phones or laptops, safe and secure and immediately report any loss or damage of their equipment to their line manager and log a security incident. If the device is a school / Trust work phone/smart phone, users must contact IT Support urgently on [nnnn nnn nnnn] to ask for the phone to be suspended.
- While at school / in the office, store the phone/laptop and associated equipment with due care. Do not leave a phone unattended on a desk and ensure your laptop is secured overnight.
- If a school / Trust device is taken home secure them as if is a personal possession. Do not lend the phone or laptop to anyone else.
- Protect school / Trust equipment appropriately when travelling, for example:
  - Laptops must always be carried as hand luggage
  - Never leave a portable device visible in parked vehicles
  - Never leave equipment unattended in a public place, for example on public transport

- Return all school / Trust assets when leaving the school / Trust. Failure to return equipment could lead to steps being taken to recover the cost, which could include legal action through the civil courts. Line Managers must complete all appropriate exit procedures with leavers. See the school / Trust onboarding / offboarding procedures for instructions.

Proven breaches of these security requirements, which are defined in the school Information Security Policy, may lead to action being taken under the school Disciplinary Procedure.

#### 4.2 User IDs and passwords

Users must:

- Protect usernames, staff numbers, and passwords appropriately.
- Create secure passwords in accordance with the school / Trust's [Information Security Policy].
- Passwords must not be stored in shared folders or written down.
- Not log on to any school / trust systems or services using another user's credentials.
- Lock a device / screen when leaving a system or service for short periods, such as taking a break during a working day.
- Log out /shut down all school / trust systems and services connected to the school / trust internal network during non-working hours, such as at the end of the working day.

#### 4.3 Unacceptable use of systems and services

Every user of school / trust systems and services must ensure that all electronic communications activities are illegal, inappropriate nor contrary to the good conduct of school business. To ensure compliance it is school policy to prohibit certain activities. Users must not use the school systems and services to:

- Create, review or transmit material that is inappropriate, offensive, untrue, defamatory, malicious, discriminatory, racist, disruptive, harassing or threatening in nature.
- Spread gossip, send chain mail letters, or copy or send material in breach of copyright.
- Download programs or any other software from the Internet.
- Create, review or transmit jokes, stories or cartoons.
- Open any e-mails which do not appear to be related to school business and seem to contain jokes, graphics, or images as such e-mails regularly contain viruses, or
- Play computer games.

Although the school acknowledges that users are often unable to control the flow of emails and Internet transmissions / webpages, users have a responsibility to ensure that inappropriate or offensive communications are deleted from systems and services. End use devices, such as desktops can be used and screens viewed by anyone, so it is essential that users are aware of their roles and responsibilities in terms of use of school / trust systems and services and comply with this AUP.

Any complaints or allegations of misuse and misconduct may be dealt with in accordance with the school's disciplinary procedure.

Appendix One provides further details of what the school deems to be unacceptable use of electronic communications, systems and services.

#### 4.4 Procurement

The school has detailed procedures to be followed when procuring electronic communications, systems and services relating to both teaching and administration. Security of systems and services and the data managed by them is a crucial aspect of the procurement of electronic communications, systems and services.

Goods and services may be purchased via the school systems and services. Where any goods/services are purchased over the Internet consideration should be given to only using a school [Pleo Card] which provides financial protection and assurances.

#### 5. Monitoring and review

This policy may be updated considering any changes in legislation or good practice and will be formally reviewed periodically.

**Review this Policy – Annually**

**Date due for review – October 2026**

## Appendix One – Unacceptable use of electronic communications, systems and services

Appendix One provides definitions of key terms and describes some key concepts relating to the use of the school / trust systems and services.

If users are in any doubt as to the appropriateness of material, they are accessing or if they are receiving inappropriate or offensive communications and material, they are to inform the school Headteacher/ as soon as possible.

It is repeated that any complaints or allegations of misuse and misconduct may be dealt with in accordance with the School Disciplinary Procedure.

### Definitions

The following definitions apply to this AUP and related school / trust policies.

#### Defamation.

Defamation is defined as the documenting of an untrue (libellous) accusation which adversely effects the professional and/or personal reputation of an individual(s) and is an offence under UK legislation. Hence it is prohibited to transmit send, access or transfer information or messages whose content or intent would reasonably be considered to be abusive, disrespectful, hurtful or undermining in nature using school/trust systems and services. The communication of information regarding alleged professional and/or personal misconduct is also to be avoided.

#### Discrimination and Harassment.

Discrimination and harassment is defined as treating a person or group less favourably than another person or group is treated, based on their age, disability, gender, race, religion/belief or sexual orientation and it cannot be shown that the treatment in question was justified.

#### Harassment.

Harassment is defined as the conduct by one person to another, which is unwanted, unreasonable and offensive to the recipient. The school is committed to the creation of a working environment free from discrimination and harassment, and this is supported by the Equality Commitment, Equal Opportunities and Harassment & Bullying Policies.

#### Inappropriate Material

The use of school facilities to knowingly create, view, read, download, upload, distribute, circulate or sell material, which is pornographic, sexually explicit, obscene, racist, sexist, violent in nature or which is criminal in nature/content is prohibited. This restriction is intended to be interpreted very widely: content may be perfectly legal in the UK yet in sufficient bad taste to fall within this prohibition. Sometimes the content may be against the law.

In general, if any user (intended to view the web page or not) might be offended by the contents of a web page, or the fact that the school software has accessed the web page might embarrass the school if made public, then it may not be viewed.

Inappropriate material also includes disclosure of private and personal information without consent.

The school will not discuss the point at which sexually explicit material may be classified as pornography. There is no personal or business justification for access to websites providing such material or for those users effecting the inward or outward, transmission of sexually explicit e-mails and/or attachments.

### Copyright

Copyright confers upon its owner exclusive rights with regard to the publication of written material and the use of computer software. These rights are enforceable in law under the Copyrights, Designs and Patents Act 1988. It is easy to attach copyright material to emails and to employ cut and paste techniques. Hence care should be taken when using these techniques. Individuals should be aware that non-compliance with the Act may result in prosecution through the courts.

It is also to be noted that staff, neither own the documents they create using school equipment, or do they have intellectual property rights therein.

### Computer Misuse

It is forbidden to use school facilities to undertake any action that is contrary to the Computer Misuse Act 1990. This Act specifies offences for attacks on computer systems and/or information. It provides protection for systems and data, attempting to maintain confidentiality, integrity and availability, and provides for three distinct offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate the commission of further offences.
- Unauthorised modification of computer material.

Protective measures against computer malicious programs (malware) have been taken by the school and users are reminded that it is prohibited to design, write, release, download, or attempt to download, any category of malware, including viruses, Trojans, worms and spyware.

### Software and Document Downloads

The school has adopted a standard desktop so that all software is correctly installed and properly licensed. It is prohibited to download programs or any other software.

If you consider that there is a business need for non-standard software please contact the relevant member of management or the IT Help Desk for advice.

Document downloads are permissible, but as such must comply with legislative requirements and are subject to the school filtering routines.

### Impersonation

It is prohibited to add, remove or modify identifying e-mail header information in an effort to deceive, mislead or fail to accurately identify the sender.

## Appendix Two – Email – Principles and Guidelines

### Principles

The school / trust email system is the primary communications system. All the general principles described in this AUP apply to the use of the school's email system, but the following points are stressed:

- Any correspondence using email represents the school.
- You should ensure that all email messages sent by you are professional in tone and content.
- The style and language of any messages, communications or information that you create should be in accordance with the school's communications policy.
- Care must be applied prior to the release of any email, or attachment, however inconsequential the contents might appear to be, to ensure that the legislative requirements and these policy standards are complied with.
- Users should only direct emails to persons who '**need to know**' the information that they contain and should only send general messages to a group of persons where it is strictly necessary to do so.
- Copying ('Cc' and 'Bcc') emails to correspondents should be kept to a minimum.
- Confirmation of receipt should be obtained for important email messages.
- The unnecessary inclusion of attachments, particularly added to messages sent internally, is also discouraged.

Email messages have the same status as any other school record and are to be treated in accordance with all associated school policies relating to topics, such as data protection and safeguarding etc. Correspondence is likely to be eligible for disclosure in response to a request for access to information under current legislation, such as the Data Protection Act 2018 and/or Freedom of Information Act 2000.

No email or other electronic transmission should be retained for longer than [3 months] unless:

- It is classified a school record and in which case its retention must comply with the school's Retention Policy.
- There is a clear business need for retention.

Hence all users must familiarise themselves with the school's [Information Management Policy / Retention Policies].

### Guidelines

To get the most out of email – be professional, efficient and protect yourself and the school-users should follow these guidelines that draw-on principles and best practice:

#### Sending email

Before deciding to send an email you should:

- Consider whether email is the most appropriate/suitable method for communication. It might be more efficient to post the planned contents of an email to a school's bulletin board and/or the intranet to make the content available to a wider audience.
- Do not congest the email system by sending trivial messages to users.

- Do not impersonate any other person when using e-mail.

In terms of the content of your emails you should:

- Pick a meaningful subject.
- Be concise.
- Answer all questions and try to pre-empt further questions.
- Make it personal.
- Keep to the message thread.
- Use templates for frequently used replies.

In terms of the style, tone and format of your emails they should:

- Unless instructed otherwise, use the school's standard font – [Arial, size 12 and black (Automatic)]
- [Have a white background rather than a colour or a personalised page.]
- Use a proper structure and layout.
- Comply with the school's policy covering accessibility
- Use proper spelling, grammar and punctuation.
- Consider whether acronyms, abbreviations and emoticons are appropriate.
- Use active voice rather than passive voice language.
- Avoid long sentences and consider the length of the email.
- Do not write in CAPITALS – use of capital letters throughout an email or in sections could be construed as 'shouting'.
- Keep your language gender neutral.
- Consider the wording used upon starting and ending the e-mail.
- [Use the school approved signature block that should include your name, details of job/role, telephone number and email address.]
- Avoid sending confidential, sensitive or personal information by e-mail.
- Never send confidential messages by e-mail without getting the recipients agreement.
- Do not send or forward emails or attachments with prohibited material.

Consider the following options when writing an email:

- Do not overuse the high priority option.
- Use the 'Cc' field sparingly by considering the need for others to receive your email.
- Always use the 'Bcc' (Blind Carbon Copy) field when emailing multiple external recipients (for example parents). This will ensure recipients cannot see each other's email addresses.
- Ensure that the e-mail has an appropriate disclaimer.
- Do not overuse the 'Reply to All' feature.
- Do not overuse 'Group' or 'All Mail User' options.
- Do not print out e-mails without considering the need for a hard copy.

And follow these instructions relating to attachments.

- Do not attach unnecessary files.
- [Wherever possible send links to documents held in a 'shared' area rather than send an attachment].

- Check that an attachment does not include any information which should not be disclosed. For example, in a hidden worksheet/s.
- Never open an e-mail attachment from an unexpected or untrustworthy source.

Finally, before sending an email:

- Check that the email address is correct, particularly when using the 'auto-fill' feature. If using the 'Bcc' field ensure that it is completed correctly. This is the largest cause of data breaches in the school. Hence pay very close attention to this point.
- Re-read the email carefully and consider the content before sending.
- Imagine that you are talking directly to the recipient.
- Consider how the recipient will interpret the message and ensure your intention is clear.
- Consider delaying the release of your email. In some email clients such as MS Outlook, you can delay the delivery of an individual message by having it held in the **Outbox** for a specified time after you click **Send**.

If you are satisfied after you have checked a draft email, then click **Send**.

Importantly, retain copies of important e-mails in accordance with the schools information management policy and retention policy.

### Managing your Inbox

Managing your Inbox/es efficiently and effectively is important. Delayed responses to requests / instructions in emails could have significant impact on the day-to-day business of the school / trust and may undermine the reputation of the school / trust. Hence, it is important that your Inbox is monitored and well managed by doing the following:

- Checking regularly for any emails and responding to / dealing with them in accordance with the school's [Communication Policy] or best practice for postal and faxed communications.
- Be cautious when reading and responding to emails – it is not difficult to fake both content and sender.
- Users should check that the content provides reasonable assurance of its authenticity and should consider checking by alternate means that it has come from the sender.
- Do not access a web site direct from an e-mail link. Instead copy and paste a link into a website into a browser first.
- For any periods of absence use the 'out of office' message feature to notify correspondents of your absence and notify them when you will return to work and what will happen to their email until your return to work. Include any alternative arrangements for dealing with emails where appropriate.
- For extend periods of absence consider diverting your Inbox to a suitably qualified co-worker or your manager.

### Replying to emails

In responding to / replying to emails you should:

- Answer them swiftly and in accordance with school's standards.
- Do not forward chain, pyramid or similar schemed emails.

- Do not copy an e-mail or attachment without careful consideration of need to do so.
- Do not forward virus hoaxes. Instead inform the school's information security lead and/or the IT Department first.
- Do not reply to unsolicited bulk e-mail, that is known as spam.
- Do not abuse others, even in response to abusive e-mails from them.
- In a reply state clearly, what is required of the recipient.
- If a recipient asks you to stop sending them personal messages, then always stop immediately.

### Deleting e-mails

Unless there is a clear need to do otherwise emails should be deleted after they have been actioned. Where there is a need to retain an email or email thread as a record it should be copied to the appropriate file store for retention as soon as possible and then deleted from the email system. The school's email system should not be used as a file store.

Key tasks to do when deleting emails:

- 'Double delete' an email/s as a minimum. This means that after deleting an email/s you must access the deleted items folder and delete them again.
- To be completely sure an e-mail is deleted you must then use the toolbar to access the option 'Recover deleted items'
- This will highlight all those e-mails you have double deleted and then you can purge these double deleted e-mails from the system so that they can no longer be recovered.

## Appendix Three - Internet Use

Users are to ensure that their use of the Internet does not affect the school in any adverse manner. If users are in any doubt as to the appropriateness of their use of the Internet, further help and advice is to be sought from senior management.

It is acknowledged that the Internet is totally unregulated and uncensored, but the school expects all Internet access to be conducted in compliance with this AUP. Failure to comply with the rules set out in the policy may result in legal claims against the user and the school and may lead to disciplinary action being taken against the user.

The costs and consequences of inappropriate use of the Internet can take many forms, but most commonly they affect the school in terms of:

- loss of productivity.
- impact on network resources.
- security issues.
- legal liability.
- adverse publicity.

## Appendix Four – Device use – Mobile phone and tablet

### Principles

Staff communicating with parents/carers, third-party suppliers and external organisation/s with school/trust devices represent the school. Hence, users should ensure that all messages and communications created are professional in tone and content. The style and language of any messages and communications that are created should be in accordance with standard business communications, see email guidelines above for some hints and tips.

Care must be applied prior to the use of mobile phones, however inconsequential the subject of the communication might appear to be, to ensure that legislative requirements and these standards are complied with.

Users should only direct communications to person who need to know the information that they contain and should only send text messages to a group of persons where it is strictly necessary to do so.

Staff must not use mobile phones in any manner that may put them, other staff or members of the public at risk.

### Guidelines

#### Device use – Mobile phone and tablet

Users must:

- Be aware of their surroundings when using a device, especially when the device is displaying information that may be considered person-identifiable, sensitive and/or confidential information.
- Always check that the person you are calling can talk safely, i.e. they may be driving or in an environment where it would be hard to maintain privacy.
- Not use a mobile phone while driving. It is an offence to do so, and they may be personally prosecuted and/or fined for doing so.
- Be aware that although the use of Bluetooth and car kits is allowable, it is not promoted. Phones should ideally be turned off while a user is driving and any messages should be retrieved at the end of the journey, when it is safe to do so.
- Disciplinary action may be taken if a member of staff uses their mobile phone in a manner that puts them, staff or the public at risk.
- Users are responsible for the day-to-day security of mobile phones issued to them:
  - Whilst in the office, store the phone and associated equipment with due care. Do not leave the phone unattended on a desk.
  - Secure it at home as if it is a personal possession. Never leave it in an unattended vehicle.
  - When not in use activate the keypad lock.
  - Set a PIN code to prevent unauthorised use (this is particularly important if you maintain any sensitive records such as contact details for vulnerable clients on the phone).

- When saving contacts onto your phone they must be saved to the sim card and not to the phone. This safeguards against phone damage as contacts are not lost with the phone, as well as allowing a smooth transfer of numbers during the upgrade process.
- When returning a phone that is no longer required all saved data, e.g. messages and contacts must be deleted, use the factory condition / reset function if available. The pin code must be set to 0000 when returning the phone or a sticker with the pin code attached to the phone.

## Appendix Five – Device use – Scanning Documents

### Principles

The principles must be followed when scanning original documentation:

- Ideally all documents that are scanned using either a Multi-Function Device (MFD) or a stand-alone scanner must be scanned and saved as a PDF and then transferred immediately to a managed storage system / service.
- Other file formats that are more suitable for storing a particular form of document, such as high-resolution photographs etc., may be used instead although before those documents are passed to external stakeholders, they should be converted to PDF.
- All relevant metadata, such as date and title, should be captured when the document is saved. No personal identifiable data should be included in the metadata.
- A scanned document must be checked against the original to ensure an accurate and complete copy.
- A scanned document must be managed in accordance with the school / Trust Retention Policy / Retention Schedule.

### Guidelines

#### Multi Functioning Devices (MFD)

The following guidelines apply to the use of MFD:

- MFDs are set to save scanned documents as a PDF. This is the default setting and cannot be changed.
- MFDs in the school are set as default to scan to a user's account that is denoted by their email address.
- Use of 'Scanned File' folders is not recommended due to and absence of access control to these folders.
- Once the document is scanned to the user's work email address, users must save the document to one of the school / Trust's managed services, such as [SharePoint] or a contracted web-service.
- Once the scanned document has been saved to a managed system / service the file containing the scanned document should be deleted.

#### Networked Devices

The following guidelines apply to the use of networked scanners to scan documents:

- Correspondence or photographs scanned via a network scanner must be scanned as a PDF.
- Drawings and plans may be scanned as a '.tif' file but must be converted to a PDF file before making them public.
- The scanned document must be indexed with the date & description in the title (metadata) and, wherever possible, a unique identifier that does not contain personal identifiable information.
- To ensure the confidentiality of scanned documents uploaded to a shared repository or application it is essential that the documents are only visible to those with proper

authorisation. Hence consideration should therefore be given to reviewing the security of the scanner functionality and application to protect the information.

### Stand-alone devices

The following guidelines apply to the use of Stand-alone devices:

- Any documents scanned via a stand-alone device must be scanned as a PDF.
- The scanned document must be saved to a managed system and must not be saved to a generic folder. The scanned document should be saved with the date & description in the title (metadata) and wherever possible a unique identifier. No personal identifiable data should be used in the document title.

### Original documents

The following guidelines apply to the original documents once they have been scanned:

- The original document should generally be destroyed after it has been scanned, to avoid duplication and minimise administration. However, in exceptional cases there may be reason/s why the document should be retained. If in doubt as to whether an original document should be kept, users should consult the Records Retention Policy, the school's business manager or the DPO.
- Thereafter the original document must be managed in accordance with Records Retention Schedules.
- All scanned documents must be checked to ensure the scanned image is an accurate and complete copy of the original source document.

Whether a document is scanned via any of the methods detailed, any further transfer of the document must be done considering the sensitivity and confidentiality of the contents of the document.

### Scanned Documents and Legal Compliance

It is important to be aware that scanned documentation may be used in legal cases, and the following describes the standing of scanned documentation under various legislation.

#### Admissibility - Civil cases

Section 8 of the Civil Evidence Act 1995 states:

##### *Proof of statements contained in documents*

*i. Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved.*

*(1) By the production of that document, or*

*(2) Whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.*

Therefore, documentary evidence in the form of electronic documents, including scanned documents, will almost always be held as legally admissible.

## Admissibility - Criminal cases

Section 71 of the Police and Criminal Evidence Act 1984 states:

*In any proceedings the contents of a document may (whether or not the document is still in existence) be proved by the production of a microfilm copy of that document or of the material part of it, authenticated in such a manner as the court may approve.*

Ultimately an original document will always hold more weight than a copy. Copies are referred to as 'secondary evidence'. However, if it can be demonstrated through robust processes and audit that a document is an authentic and true copy of the original, it will have almost the same weight as the original and it is unlikely it will be challenged.

## Admissibility – British Standard of scanned documents

British Standard is BSI 10008:2014 – Legal Admissibility and Evidential Weight of Information Stored Electronically - sets the benchmark for procedures that should be followed to achieve best practice and, therefore, the legal admissibility of electronic documents.

## Copyright

The scanning of any document for which a third party holds the copyright must comply with the Copyright, Designs & Patents Act 1988. Copyright applies equally to paper documents, electronic information, CD-ROMs, websites, images, computer programs etc.

## Appendix Six – Device Use – Personal Use of school Devices and Communication Methods

### Introduction

The hardware, software and materials relating to electronic communications are owned wholly by the school, which provides access to them to facilitate effective business communication within the workplace. As such they are provided primarily for business use.

Personal use of the school mobile phones or systems to send e-mails or to browse the Internet is permitted, but should be on a minimal basis only, and is defined below. Inappropriate or excessive use of such systems for personal use will be dealt with as a disciplinary issue.

### Guidelines

When using electronic communication systems (email, internet and mobile phone) for personal use, users are to ensure that:

- The usage is minimal and takes place substantially out of normal working hours and not at other times when the employee is expected to fulfil his/her contractual responsibility to work.
- Whenever it takes place, it does not interfere with school business commitments, adversely affect school systems or harm the school reputation.
- It does not incur any additional expense to the school. Where it does, i.e. where the school is liable for calls and text charges which relate to personal use, then these costs must be reimbursed to the school
- .
- The usage is appropriate. Personal use of mobile phones is permitted where there is an urgent matter, such as the health of themselves or immediate family or a change in working circumstances, i.e. staff need to unexpectedly work late. There is no expectation that such calls should be paid for by the individual.
- Activity complies with what is described under the heading of 'Prohibited Use'.
- Use is at your own risk and the school accepts no responsibility for any loss or disclosure of personal e-mail or attachments.
- E-mails make it clear that the opinions expressed are your own and not the school. To that effect all personal e-mails must also include at the start or sign off a disclaimer to this effect.  
*Personal email". The views, comments expressed and transaction details contained within this e-mail are personal and are not those of school. This email is the personal responsibility of the sender."*
- You do not use school facilities for any for-profit business or commercial gain.
- Non-commercial personal procurement, such as the purchase of tickets by e-mail and the use of Internet web sites, is on a minimal basis only. The use of a school email address for this purpose is to be accompanied by a disclaimer as outlined above.

Personal e-mails blocked by the school content filtering routines will not be released to the recipient. The school has implemented measures to protect the systems in accordance with this AUP and will not employ resources to the release of such emails. Business emails will continue to be released upon request, once proof of business content and need has been established.

If in doubt as to whether the intended use is permissible, advice should be sought from the IT provider, senior management or DPO before proceeding.

In respect of the Data Protection Act 2018, employees using the Internet for personal purposes are Data Controllers in respect to the processing of personal information. As Data Controllers in these circumstances, employees are responsible for ensuring that personal data is processed in line with the principles of the Act.

Any complaints or allegations of misuse and misconduct may be dealt with in accordance with the school's disciplinary procedure/s.

## Appendix Seven - Social Media

### Introduction

Social media is the term commonly given to websites, online tools and other interactive digital tools that allows users to interact with each other, by sharing information, opinions knowledge and interests. These include:

- Social networking utilities, such as Facebook, Instagram, X (formerly Twitter)
- Online discussion forums.
- Collaborative spaces
- Media sharing services, such as Flickr and YouTube
- Blogs, (personal Web Logs), such as Blogger
- Microblogging applications, such X, Bluesky and Reddit.

It is important that everyone uses the technologies and services effectively, flexibly and in an appropriate manner. While at work and at home users must act in a way that does not compromise the school's reputation.

All users should bear in mind that information they share through social media applications, even if they are on private spaces, is still subject to:

- Copyright, Designs & Patents Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- The school Equal Opportunities Policy.

### Principles

When using social media in a private and personal capacity users should also follow the principles suggested by the social media sites for their own safety. These can normally be found on the information pages of each social media site. Those general guidelines include:

- Taking care how users are perceived, as the boundaries between their professional life and private life can become blurred in social networks.
- Considering whether users would be happy for their colleagues, managers or service users to read the comments, and consider what their reaction might be.
- Showing respect for others. You should be respectful of the school and your fellow staff and volunteers.
- Ensuring that the privacy of others is always respected.
- Obtain the permission of individuals before posting contact details or pictures.
- Not use sites for accessing or sharing illegal content; and
- Use social media in a responsible fashion and avoid giving out personal information about you or your family.

## Guidelines

### Authorised users of social media

Social media is to be used on behalf of the school only by:

- Those people who have been identified as media spokespeople by the Headteacher
- Those with another defined role that have been appropriately trained. These roles should be defined in a business case that is supported by a member of the senior leadership team / head of department.
- Users who have been given responsibility as part of managing an emergency.

For those people authorised to respond on behalf of the school, training will be provided. Although social media is more conversational than other forms of communication it should be treated in an equally professional way.

Where authorised individuals from key partners and/or external organisations are authorised to act on behalf of the school, they will also be expected to comply with all relevant school policies and associated guidelines.

Staff authorised to speak on behalf of the school should ensure that they comply with set out in the next section and all other legal requirements.

Those people who wish to respond in their own personal and private capacity should ensure that they comply with the guidelines in the appropriate section below.

### Access to social media sites

Social media sites are currently blocked when using school desktops and laptops but can be made available subject to approval.

### Restrictions on the use of social media

While using social media on behalf of the school, users must not:

- Publish any content that may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Be used for party political purposes or specific campaigning purposes.
- Be used for the promotion of personal financial interests, commercial ventures, or personal campaigns.
- Be used in an abusive or hateful manner.
- Be used for actions that would put school users in breach of school codes of conduct or policies.
- Breach the school misconduct, equal opportunities or bullying and harassment policies.
- To release information that could be considered confidential; or
- Damage the school reputation.

## Correct use of social media for school business

It is also important that members of the public and other users of online services know when a social media application is being used for official school purposes. To assist with this, all users must adhere to the following guidelines:

- All links should be to the school website or other approved sites.
- The school domain email address should be used for official school purposes, unless otherwise agreed by the relevant school Headteacher.
- The use of the school logo and other branding elements should be used where appropriate to indicate the school support or where the school responds formally.
- The logo should not be used on social media applications which are unrelated to or are not representative of the school official position.
- Staff representing the school should identify themselves as such where appropriate – on social media applications i.e. through providing additional information in user profiles. It is not considered appropriate for school officers acting on behalf of the school to deceive, even inadvertently, other users of social media.
- They should ensure that any contributions they make are professional and uphold the reputation of the school.
- Comply with all the relevant legislation and the school policies on IT.
- They must not promote or comment on political matters or issues that may be regarded as such.
- Avoid endorsements that are not relevant to the operation the school.
- Be aware that all information that you post on behalf of the school may be subject to the Freedom of Information Act.

## Using social media in a private and personal capacity

The school understands that staff may use social media, on their own equipment in their own time, for their own private use. Before posting comments, staff should always remember that information posted on these websites becomes public knowledge and may be viewed by colleagues, service users, members of the public and the press.

These guidelines do not mean that staff can never post comments on these websites about their work for the school. The school routinely monitors comments made about it, in social media.

Staff must not connect with current pupils on social media. Staff may wish to mask or edit their username to hinder pupils locating them on social media platforms. For more information see the school E-Safety and Safeguarding Policies.

Unless staff are authorised to speak on behalf of the school, outside of their work time they should:

- Use a disclaimer to make it clear that their views are their own and not necessarily those of the school.
- Avoid any actions that would put school users in breach of school codes of conduct or policies.
- Avoid publishing or passing on links to any defamatory and/or knowingly false material about the school, your colleagues and/or customers

- Avoid using language that could be deemed offensive to others.
- Not breach the school misconduct, equal opportunities or bullying and harassment policies.
- Not reveal confidential information relating to his/her employment within the school.
- Not say anything that would damage the school's reputation.

### Using social media in connection with vulnerable people

There will be additional requirements when dealing with particularly vulnerable groups and you should also refer to any additional guidance that has produced in these instances.

Staff working with vulnerable people will need to be especially vigilant and undertake safe on-line behaviour.

Management may issue specific guidelines or codes of conduct to meet individual concerns related to the nature of their area.

### Breaches of these guidelines

The school takes appropriate and safe use of social media very seriously and any breach of this policy could lead to disciplinary action.

If it is believed that the school has been brought into disrepute this may constitute misconduct or gross misconduct, and disciplinary action will be applied as appropriate.