Blythe Bridge High School & Sixth Form
ICT Security & Acceptable Use Policy

This policy applies to all schools, all staff, students, and governors as well as guest users at Blythe Bridge High School & Sixth Form.

The objectives of the Policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.
- To specify minimum standards that constitute acceptable use of ICT systems.

'Information' covers any information, including electronic capture and storage, manual paperrecords, video and audio recordings and any images, however created. The school's Senior Network Technician is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. The Senior Network Technician will be the official point of contact for ICT or information security issues.

Responsibilities:

- Users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy
- Users are responsible for notifying the Senior Network Technician or Business & Operations Manager of any suspected or actual breach of ICT security; a log of security or privacy breaches will be made in the relevant register, to comply with GDPR.
- Users must comply with the requirements of the Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act1984.

- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.

Procedural Aspects of the Policy

- The **Governing Body** must ensure that the school implements an ICT Security Policy. This must be reviewed annually.
- The **Headteacher** must nominate a Senior Network Technician or members of non- teaching staff with designated systems management responsibilities. This must be documented and included in the Scheme of Delegation approved by the Governing Body.

  The Headteacher must ensure that the nominated member(s) of non-teaching staff understands the functions of the role and is familiar with the relevant Acts.
- The **Headteacher** must compile a census of data giving details and usage of all personal data held on computer and manually (as required under GDPR) in the school, and file a registration with the Data Protection Registrar. Users should be periodically remindedof the requirements of the Data Protection Act, particularly the limitations on the storage and disclosure of information.
- The **Senior Network Technician** should ensure that a copy of the relevant Acceptable Use Policy is made available to all users and that users are periodically reminded of their obligations under this policy. This should include all relevant aspects of the ICT Security Policy and any other information on the use of facilities and techniques to protect the systems or data.
- The **Senior Network Technician** should retain a record of
  - the access rights to systems and data granted to individual users;
  - any amendments or withdrawal of these rights due to a change in responsibilities or termination of employment or starters/leavers;
  - the training provided to groups and individual users.
- An inventory of all ICT equipment must be maintained and regularly updated by the **Senior Network Technician** (or ICT support staff where the processing of equipment in/equipment out has been delegated by the Senior Network Technician) as equipment is purchased/disposed of. The inventory must be checked and verified annually in accordance with the requirements

  of financial regulations. The Senior Network Technician must ensure there are clear procedures regarding the disposal of equipment containing confidential or sensitive data; such procedures must be compliant with the Waste from Electronic and Electrical Equipment (WEEE) directive and that that third parties involved in the disposal of equipment are registered under the Data Protection Act as personnel authorised to see data; as such they will be bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

- An inventory of all software and licence details must be maintained and regularly updated by the **Senior Network Technician** as software is purchased/disposed of. The inventory must be checked annually to ensure that the licences accord with installations.
- The **Senior Network Technician** should ensure there are clear procedures regarding the installing/copying of software. The Senior Network Technician should be familiar with the requirements of FAST (the Federation Against Software Theft) and industry best practice.
- The **Senior Network Technician** should periodically undertake a 'password strength checking exercise' to identify any weak passwords being used by staff to protect sensitive data and rectify security weaknesses as soon as possible; the frequency of such exercises will be

  determined through threat analysis decided at departmental review with the Executive Headteacher.
- The **Senior Network Technician** must ensure that "shared passwords" – such as those used by ICT support staff to administer school servers, are
  - sufficiently complex to satisfy industry best practice on security
  - stored in password management software that utilises strong encryption
- The **Senior Network Technician** should devise and implement a policy on anti-virus software for local networks, stand-alone systems, laptops and privately-owned devices used to access school networks. This must ensure that antivirus software is regularly updated, suitable for the task of identifying malware and protecting school systems and data from malware attacks.

Backup Strategy

Backups are taken for the purposes of disaster recovery; they are not intended as a method to recover work lost by individual students through user error. All data is backed up every night using an incremental strategy. Once a week, all data is backed up in full; this is kept until backup storage capacity necessitates an overwrite which is usually 9-12 months and never less than 6 months.
All backups are kept in a remote location.

All backups are checked to ensure that they have been successful. The backup mechanism is tested once a year in a virtualised environment to check its reliability.

'Bring Your Own Device' Policy

Blythe Bridge High School & Sixth Form grants its sixth form students and employees the privilege of using smartphones and tablets of their choosing at school for their convenience, subject to relevant Mobile Phone Policies in place. Blythe Bridge High School & Sixth Form reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined herein. This policy is intended to protect the security and integrity of Blythe Bridge High School & Sixth Form's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. Blythe Bridge High School & Sixth Form employees and students must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the school network.

Acceptable Use

- The school defines acceptable use as activities that directly or indirectly support the students' education.
- The school defines acceptable personal use during work time as reasonable and limited personal communication or recreation.
- Employees and students are blocked from accessing certain websites during work hours/while connected to the school network at the discretion of the Senior Network Technician and Headteacher.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in external business activities

Employees and Sixth Form students may use their mobile device to access the following school-owned resources: email, calendars, contacts, documents and software packages (where licensing restrictions permit).

Devices and Support

- Smartphones including iPhone, Android and Windows phones are allowed, subject to restrictions in the school's Mobile Phone Policy. Tablets including iPad, Android and Windows Surface are allowed.
- Connectivity issues are supported by ICT; employees and students should contact the device manufacturer or their carrier for operating system or hardware-related issues. ICT support staff will assist staff and Sixth Form students in configuring devices to connect to school wifi access points.

Security

- In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the school's network. Password complexity is referenced in Password policy
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Employees' and students' access to school data will be limited, based on user profiles defined by ICT and automatically enforced.

Risks/Liabilities/Disclaimers

- The schools reserve the right to disconnect devices or disable services without notification.
- Lost or stolen devices owned by the school must be reported to the ICT helpdesk soon as possible. Privately-owned devices that contain data owned by the school that have subsequently been lost, must also be reported to ICT.
- The employee or student is expected to use his or her devices in an ethical manner at all times and adhere to the Acceptable Use Policy.
- The employee or student is personally liable for all costs associated with his or her device.
- The employee or student assumes full liability for risks including, but not limited to, the partial or complete loss of school and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Blythe Bridge High School & Sixth Form reserves the right to take appropriate disciplinary action.

Security & safety requirements for ICT systems

Password policy

Blythe Bridge High School & Sixth Form will enforce a policy of strong passwords for all staff users and users with elevated privileges, on the grounds that they regularly have access to sensitive personal information. Staff passwords should be:

- at least 10 characters in length

Passwords should never be:

- written down
- easy to guess

ICT staff will periodically undertake password security exercises where staff and student passwords will be subjected to security testing procedures for the purposes of identifying users with weak passwords and protecting school systems from unauthorised access by third parties who might seek to exploit users' weak passwords. Staff users will be required to change their password(s) in situations where periodic security testing identifies that weak passwords have been used, or where it is known or suspected that a user's password may have been compromised by unauthorised third parties.

Unattended workstations

Staff screensavers will lock with a password after 60 minutes of inactivity . Staff must be mindful of what is being displayed on their screen and who can see it; leaving unlocked workstations with sensitive data such as email or SIMS applications active must be avoided

Portable media

- Portable media such as USB devices may be used to transport files between home and school.
- Any files containing personal information or other sensitive data may only be transported outside the Blythe Bridge High School & Sixth Form on encrypted devices.
- When disposing of legacy portable hardware that may not have been encrypted in the past, staff should seek advice from the ICT support staff to ensure that any sensitive data is securely erased.
- As an alternative to portable media, staff are encouraged to make use of remote desktop connections and their school OneDrive account, which prevent the need to transport sensitive data on physical devices.

File-type & software restrictions

The Senior Network Technician will ensure appropriate security policies are in place to prevent unauthorisedusers from using file types that could bypass security measures or otherwise cause security problems. This includes but is not limited to: preventing the execution of non-whitelisted executable files or shell scripts; preventing the download of executable or software package files or harmful office macros.

Physical security

As far as practicable, only authorised persons will be admitted to rooms that contain servers or provide access to data. Server rooms must be kept locked when unattended. Uninterruptible Power Supply (UPS) units will be used for servers and network cabinets.

Internet use & filtering

The Senior Network Technician will ensure that appropriate firewalls are in use at the extremities of the school networks to guard against nefarious actors gaining unauthorised access to school systems. Filtering proxy servers will also be used to ensure that all internet traffic is age-appropriate, safe to use and logged. Where staff or students become aware of inappropriate material being accessed on school systems, this should be reported to the ICT helpdesk: IT@bb-hs.co.uk. Social mediaincluding but not limited to Facebook & Twitter will be blocked for all high school students. Non-approved email systems such as Hotmail will be blocked to prevent cyberbullying and access to unauthorised materials. The school Acceptable Use Policy (AUP) is available as part of this document for staff andstudents; all persons using the network will be required to accept the AUP before they logon.

Parental permission will be required before any student is allowed to use school ICT facilities; this is managed through the home-school agreements and pre-admission procedures for each school.

Monitoring system usage

Blythe Bridge High School & Sixth Form is mindful of its obligations in regard to the monitoring of data on school networks and the potential for monitoring activity to contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act, 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. ICT support staff will be mindful of their obligations under law, including the Data Protection Act (2018) which incorporated the General Data Protection Regulations (GDPR) into UK law; monitoring of ICT system use for school business will be reasonable and proportionate, the purposes of protecting students from harm; complying with the law; and preventing unauthorised access to school ICT systems or private information.

In order to facilitate the monitoring of internet traffic passing through Blythe Bridge High School & Sixth Form systems, ICT staff may deploy TLS certificate systems to act as 'man in the middle' providers when users access encrypted web traffic using the HTTPS protocol. Web browsers on school-operated devices will have the appropriate TLS certificate-signing authorities pre-installed and 'trusted' to facilitate such monitoring and this will be disclosed to users in the AUP. The school may only monitor authorised private use of a school computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of the protection of well-being or for the protection of the rights andfreedoms of others. The Senior Network Technician should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place. Users should be aware that the protocols discussed here in Monitoring system usage apply to all internet traffic at all times on CHFS workstations. Users will be informed that all ICT system usage is monitored as part of the AUP.

Rules for ICT use by third parties

Under some circumstances, it may be desirable to grant third parties (that is, people who are neither staff, governors or students) access to school ICT systems, such as ICT service providers, potential staff attending interview or pre-employment induction, or potential students.

In general,

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own securearea or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in access privileges being revoked and could be used to inform decisions about potential employment or acceptance in the case of candidates for employment or admission.

Guidance for best practice for staff communication is included in the appendix: E-mail & Internet use good practice for staff and for Classroom monitoring of students' ICT usage, as is the Acceptable Use Policy.

Appendix

Acceptable Use Policy

This Acceptable Use Policy (AUP) applies to all users of ICT systems at Blythe Bridge High School & Sixth Form. In consenting to use ICT systems operated by Blythe Bridge High School & Sixth Form, or connecting to systems operated by Blythe Bridge High School & Sixth Form using privately-owned devices, all users agree to follow the best practices outlined below. Prior to logging in to Blythe Bridge High School & Sixth Form -owned workstations, users are required to confirm their compliance with and acceptance of the AUP.

At all times, users will act in good faith to maintain the security and privacy of school ICT systems and users' private data. Users agree to comply with any obligations outlined in the ICT Security Policy.

Students are required to accept and comply with the student usage particulars, that they will:

- only use their own login and password, and keep their password secret
- only use the computers for school related study
- be responsible for their own files and understand that the school will check files and monitor the websites visited
- only contact people they know or those whom the teacher has approved of
- will not give out any personal information such as mobile phone numbers or addresses, or arrange to meet strangers; report any contact from people outside of school immediately to an adult
- only enter sites on the internet that have been authorised by the teacher; not enter social media websites or play internet games
- only store files for school use on the network
- not plagiarise other pupils' electronic work or by using the internet

Staff agree that:
They will protect private information held in their capacity as an employee of the school, making use of confidential waste bins to dispose of printed media and adhering to the requirements in the ICT Security Policy for electronic media. Their use of ICT systems will be legal, in compliance with all school policies and for the purposes of their job role.

All users accept that their usage of systems may be monitored and in particular that 'man in the middle'-style encryption interception may be used to ensure website access is compliant with the school's filtering of illicit content. Users understand and accept the principles of monitoring covered in the ICT Security Policy.

Classroom monitoring of students' ICT usage

Staff should ensure they are able to visually monitor pupils' use of computers at school and that there is always a responsible person present. Monitoring software such as Impero may be used to facilitate in-lesson monitoring by teaching staff. ICT will log access to the network using software tools, and in particular, logs of network and internet traffic will be kept for the purposes of generating an audit trail of student and staff ICT usage.

Where staff or students' use of ICT systems could constitute illegal activity, staff are duty bound to bring this to the attention of the Headteacher or other members of the Senior LeadershipTeam so that appropriate action can be taken; where staff identify activity that constitutes a safeguarding concern, they must immediately raise this with the Designated Safeguarding Lead.

E-mail & Internet use good practice for staff

The following guidelines (some of which also apply to other forms of correspondence) advise what is and what is not good practice when using e-mail and other similar systems to communicate.

Staff should:

- treat E-mail as they would a letter, remembering that they can be forwarded/ copied to others;
- only contact children for professional reasons and in accordance with school policy;
- use "BCC" fields when addressing emails to multiple recipients whose confidentiality needs to be maintained.

Staff should not:

- use internet or web-based communication channels to send students messages of a 'personal' nature
- use or access social networking sites of children or young people
- use internet or web-based social media channels to bring Staffordshire County Council or the school's name into disrepute;

Virtual Learning Environment (FROG) Acceptable Use Policy

The following policy outlines the terms of use for all users (staff and students) of Blythe Bridge High School & Sixth Form’s virtual learning environment (Frog).
All Blythe Bridge High School & Sixth Form staff and students are granted access to Frog to facilitate learning and teaching. Access is conditional upon agreement with school regulations and all relevant UK laws.
Failure to comply may result in loss of privileges. In cases where UK law has been violated, users could face criminal and/or civil liability.

Acceptable Use

Blythe Bridge High School & Sixth Form expects and requires that its users act responsibly and considerately, and respect the rights of other Frog users at all times.

Unacceptable Use

Any users that infringe the policy, behave inappropriately online, or adversely affect Blythe Bridge High School & Sixth Form's online learning communities will be denied access to Frog. The following constitutes unacceptable use of Frog:

1. Unauthorised use of another person’s login details to gain access to the Frog system.
2. Unauthorised reading, copying, modification, or corruption of another users files, communications, or data.
3. Attempts to undermine the security or integrity of Frog and related systems/software.
4. Posting or using material that infringes copyright and intellectual property rights. If you are unsure whether Blythe Bridge High School & Sixth Form owns a particular licence to reproduce materials, you should contact the Senior ICT Technician or Business Manager for confirmation.
5. Creation or transmission of any materials that are considered offensive, obscene, or indecent.
6. Creation and transmission of materials/communications that include profanity, vulgarity, hate speech, disruptive or hostile comments, interpersonal disputes, or threats of violence.
7. Discussing or re-posting materials/communications that have been deemed inappropriate and removed by the school.
8. Creation and transmission of materials, or taking actions, that interfere with Frog operations.
9. Including another user’s contact details or personal information in materials/communications without express permission from the individual concerned.
10. Refusing to adhere to the schools IT and conduct policies, procedures and agreements.
11. Using Frog for commercial purposes or financial gain without express approval from Blythe Bridge High School & Sixth Form.
12. Violating the privacy and confidentiality of other users.

Additional Notes

- All users are responsible for their activities on the Frog system and for the content of their uploaded materials and communications (via chat rooms, email or discussion forums).
- The school aims to remove any inappropriate materials as soon as possible after they are discovered or reported and will deal with inappropriate use or behaviour of Frog swiftly and rigorously within the guidelines of the school's disciplinary procedures.

Social Media Code of Conduct Policy

1 Introduction

This code of practice provides employees with guidance to ensure that they are taking the necessary steps to protect themselves and others against cyber bullying.

It also provides employees with practical guidance on how they can ensure that their conduct in relation to social networking sites and electronic media is accordance with the code of conduct for all Local Government employees as interpreted by Staffordshire County Council in relation to social networking sites and electronic media.

1.1 Guidelines for Social Networking

Online communities can help Blythe Bridge High School & Sixth Form connect with its stakeholders in many ways. At the same time, there are some cautionary lessons that have emerged from participating in online communities. Participants should take note of the following:

- You are legally liable for anything you write or present online. Employees and students can be disciplined by the school for commentary, content, or images that are defamatory, pornographic, proprietary, harassing or that can create a hostile work environment. You can also be sued by School employees, competitors, and any individual or company that views your commentary, content or images as defamatory, pornographic, proprietary, harassing or creating a hostile work environment. No written comment should be made that could be offensive to anyone in any of the seven Equality and Diversity strands: age, disability, gender/transgender, religion or belief, sexual orientation, socio-economic group.
- You are posting content onto the World Wide Web and cannot ensure who does and does not have access to your information.
- Information you post online may continue to stay on the World Wide Web even after you erase or delete that information from pages.
- Before participating in any online community understand that anything posted online is available to anyone in the world.
- Do not post information, photos or other items online that could reflect negatively on you, your family or Blythe Bridge High School & Sixth Form.
- Be discreet, respectful, gracious and as accurate as you can be in any comments or content you post online.

Staff are also referred to the Safeguarding Policy which reminds them that any form of personal relationship between staff and students who are under 18 years of age or are vulnerable adults, is expressly forbidden. This would include any form of personal conversation or comment through the medium of the Internet. Therefore, Staff should not be 'Facebook friends' with any students. If a staff member discovers an imposter account has been made in their name they should report it immediately.

1.2 Guidelines for Blogging

If teaching staff and/or a student own a blogging site the following guidelines should apply.

- Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the School. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the School.
- Information published on your blog should comply with the School policies. This also applies to comments posted on other blogs, forums and social networking sites.
- Be respectful to the School's other employees, students and competitors.
- Social media activities should not interfere with work commitments.
- Your online presence reflects the School. Be aware that your actions captured via images, posts, or comments can reflect that of the School.
- Do not reference School employees or partners without their express consent.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Company logos and trademarks may not be used without the written consent of the Business Manager as set out below.

2.1 Cyber Bullying

Definition: "Cyber bullying is the use of Information and Communications Technology (ICT), particularly mobile phones and internet, deliberately to upset someone else"
[Cyber bullying: Guidance issued by the DCSF 2007]

Staffordshire County Council supports the view that cyber bullying represents a cruel, dangerous and inescapable form of bullying that causes humiliation, stress and trauma to its victims, and so believes that cyber bullying is not acceptable and will not be tolerated.

Blythe Bridge High School & Sixth Form are committed to the view that cyber bullying is never acceptable and is not tolerated

2.2 Legislation

Although bullying is not a specific criminal offence, criminal law exists to prevent certain behaviours. These behaviours may constitute harassment, or cause a fear of violence. Sending indecent, grossly offensive or threatening letters, electronic communications or other articles to another person is illegal

Other legislation protects against the publication of obscene articles or data (e.g. over a school intranet), hacking into someone else's computer, invading their privacy, damaging their reputation or engaging in anti-social acts.

2.3 Protecting yourself against Cyber Bullying

There are simple measures that you can take to safeguard against cyber bullying:

- being careful about personal information and images posted on the internet
- not leaving your mobile phone or personal computer around for others to gain access or leaving details on view when left unattended
- choosing hard-to-guess passwords and not letting anyone else know them being aware of the risks of giving your mobile number or personal e-mail address to others
- making use of blocking facilities made available by website and service providers
- not replying or retaliating to a bullying message
- saving evidence of offending messages
- making sure you inform others of any mobile phone or online bullying or harassment in accordance with relevant policies.

2.4 What action you can take

- Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. Cyber bullying
- Complaints will be investigated to obtain any evidence available and you can support this process by:
- Logging any incidents
- Noting the dates, times and content of messages and, where possible, the sender's identity or web address.

Taking an accurate copy of the whole web page address, for example, helps service providers to locate offending material. Such evidence may be required also to show to those who need to know, including police.
Saving evidence of texts and images on the device itself is useful. It is important they are not deleted.

In the non work environment it may be appropriate to report incidents of cyber bullying direct to an internet service provider or mobile phone company. Content may be blocked and / or removed if it is illegal or breaks the provider's own terms and conditions. Some providers issue conduct warnings to users and are able to delete the accounts of those who have broken the rules.

3. Safeguarding

In order to safeguard yourself and potentially vulnerable adults and young people who you may work with you should ensure that your behaviour with regard to social networking sites is consistent with the standards of behaviour expected in normal day to day interactions with vulnerable adults and young people.

Communication that is undertaken via social networking sites is comparable to 'one to one' interaction in other contexts, and individuals should avoid any activity which would lead any reasonable person to question their motivation and intentions.

You are reminded that it is expected that you:

a) Always act in such a way as to promote and safeguard the well being and interests of service users and colleagues.

b) Take all reasonable steps to ensure that relationships with service users and colleagues are such that there can be no suggestion of impropriety whether by word or action.

c) Develop a friendly relationship between employee and service users, with clear boundaries. It is deemed an abuse of that professional relationship for an employee:

- to enter into an improper relationship with a service user
- to show favour towards a particular service user
- to act in a threatening or aggressive manner or to use foul, abusive or profane language
- to endeavour to exert an undue influence with regard to personal attitudes, opinions or behaviour which is in no way connected to the work of the Service.

d) Take all reasonable steps to ensure that no action or omission on your part or within your sphere of influence is detrimental to the condition or safety of service users

In order to preserve these standards of behaviour it is recommended that you decline any request from an existing or previous service user to be a "friend" on your Social Network Site.

It is inappropriate to request contact with an existing or previous user of the service via this medium or any other form of electronic medium.

It is acknowledged that you may accept a service user as a "friend" unintentionally and where this occurs you are advised to ensure that you remove this access as soon as you become aware of their status. You should do this in a way that does not jeopardise your professional relationship and should inform your Line Manager, if any significant conversation or activity occurs.

All employees are advised to ensure that when setting up social networking sites they should make full use of the range of tools which enable the access to personal information to be restricted.

4 Conclusion

Where no guidelines exist, staff should use their professional judgement and take the most prudent action possible. Consult with the School’s Business Manager if you are uncertain.

Media contacts about the School, our students, employees, partners, customers and competitors must be referred for co-ordination and guidance to the Director of Business & Finance.

Please note that any activity on School’s internal systems are monitored and recorded. Any external web activity is monitored, recorded and filtered whilst accessed on the school network.

The breach of Social Media Code of Conduct and any content that would adversely affect the School could result in a disciplinary action.