POLICY STATEMENT

Policy	Online safety and Acceptable Use of I.T. Policy
Department	Administration
Date Written	September 2018
Written by	Michael Lawless, Di Durrant and Brendan Commane
Approved by	Kevin Samson
Date of Approval	14 September 2018
Next major review date	14th August 2019
Location and disseminations	A copy of the policy can be found in staff handbook, in the school foyer and on the school website.
The context of the policy and its relationship to other policies	This policy should be considered in conjunction with other written policies on behaviour, health and safety, medicines, healthy schools, school visits and child protection.

1. Policy Statement

Buckswood School aim to support the full use of the vast educational potential of new technologies together with our responsibility to provide safeguards against risk, unacceptable material and activities. This policy and the guidelines within it aim to protect staff from e-safety incidents and promote a safe e-learning environment.

The School's ICT and related systems are important and essential assets which need to be appropriately protected. The School is concerned with establishing a framework of acceptable usage and controls, including staff responsibilities, in order to safeguard our ICT hardware, systems, infrastructure and data from:

- unauthorised access
- accidental or intentional damage
- interruptions to availability of services
- use for illegal purposes

At Buckswood we believe that staff should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

This policy applies to the use of technology on School premises and also any use, whether on or off School premises, which affects the welfare of other pupils or where the culture or reputation of the School are put at risk

The aims of this policy are two fold:

(1) in relation to acceptable use of IT to:

- encourage staff and students to make good use of educational opportunities presented by access to the Internet and electronic communication
- to safeguard and promote the welfare of pupils by preventing "cyberbullying" and other forms of abuse
- minimise the risk of harm to the assets and reputation of the School
- help staff take responsibility for their own e-safety
- ensure that staff use technology safely and securely

(2) In relation to online Safety Buckswood recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e- safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online*.*

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children.

The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential.

This policy aims to regulate ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our Cyber Bullying and Behaviour Policies.

For more information on data protection see also data protection policy.

2. Roles and Responsibilities

The Principals have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinator. Any complaint about staff misuse must be referred to the online safety coordinator at the school or, in the case of a serious complaint, to the Proprietor.

The Principals will:

- Ensure access to induction and training in online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured, in accordance with the GDPR.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- The Senior Management Team will receive monitoring reports from the ICT Manager.
- Ensure weekly Smoothwall reports are taken of usage and results shared with the Principal. These results will be used to track patterns of inappropriate use.

The Online Safety Coordinator will:

- Leads online-safety meetings every ½ term.
- Reports to SMT, via the e-safety committee

The ICT Manager is responsible for ensuring:

- That the school’s technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal; online safety coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.

3. Health & Safety

The hazards associated with computing are relatively minor and are assessed by the Health and Safety Officer in accordance with all relevant legislation and guidance. Much of the legislation concerning the use of equipment, ergonomic considerations, eye tests etc. are not applicable to ‘occasional’ PC/computer users.

4. Confidentiality

Every effort is made to protect the security and confidentiality of information stored on the School’s networks. This has to be balanced against the School's responsibility to maintain internal rules and regulations and to comply with any relevant laws.

5. Copyright

The ownership of work produced by staff and pupils can sometimes be in doubt. The School's policy is to interpret the law as generously as possible in favour of the author while retaining the rights only to such items as are covered specifically by this policy.

6. Computer Misuse Act

The unauthorised use of computers is a criminal offence. The Computer Misuse Act of 1990 formalises this and explains the different offences and penalties.

7. Use of Personal Equipment on the School Network

Use of personal devices, for example smart phones or tablets etc, on the school filtered network is permitted but the school is not responsible for the loss or damage of equipment.

Personal devices should have no unlicensed or illegally copied software (including music and other data files) on it and you should be aware that you are still using school network systems to connect to the internet.

8. Acceptable Usage Policy

This policy applies to all non-pupil/student users of the School's IT facilities and sets down the standards which users are required to observe in the use of the IT network, email and the internet.

Non-pupil/student users include teaching and support staff, visiting adults and any other user category not defined as a pupil/student of the school.

Access for non-school related purposes is provided on a best effort's basis and subject to normal security and firewall rules. Buckswood School cannot compromise network security to accommodate personal preferences or requirements.

Deliberate access of inappropriate material by employees or visitors through school systems would be regarded by the school as a significant breach of trust, or, for certain materials or sites, gross misconduct, which may result in the school taking disciplinary action.

It is the responsibility of all users to acquaint themselves and comply with this policy.

Certain terms in this policy should be understood expansively to include related concepts.

School includes all Buckswood School locations and both academic and non-academic areas.

Document covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the HTML files read in an internet browser, any file meant to be accessed by a word processing or desk-top publishing programme or its viewer or any other electronic publishing tools.

Graphics includes photographs, pictures, animations, movies or drawings.

Display includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-reality tools.

The acceptable usage policy is split into seven sections:

- Internet
- Contacting Pupils/Students Email
- Security
- Copyright
- Use of Technology in Classrooms
- Audio and Visual

By logging on to the Buckswood School network you signify your acceptance of this policy, and you should seek clarification of any issues that you do not understand.

9. Internet

Use of the Internet by non-pupil/student users is permitted and encouraged where such use is suitable for school purposes and supports Buckswood School's aims and is used in a manner which is consistent with Buckswood School's standards of professional business conduct.

During School hours, we expect you to restrict your Internet usage to School related purposes only or to use the facilities in such a way as not to impact on overall performance – for instance, not to download large files or use streaming media excessively.

All existing School policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with privacy, misuse of School resources, sexual harassment, fraud and information security and cyberbullying.

Any file, including e-mails, that is uploaded or downloaded must be scanned for viruses before it is run or accessed. This should be done automatically, so non-pupil/student users must check that their antivirus software is running. Ask for advice from the IT department if you are unsure how to do this.

The School's internet facilities and computing resources must not be used knowingly to break the law. Use of any School resources for illegal activity is grounds for immediate action and the School will co-operate with any legitimate law enforcement agency. Please see section 16.

Any legal and licensed software or files downloaded via the Internet into the School network become the property of Buckswood School. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

- No user may use School facilities knowingly to download or distribute pirated (illegal and unlicensed) software or data.
- No user may use the School's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the security of staff or pupils/students.
- No user may use the School's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door programme code.

Non-pupil users are specifically prohibited from downloading any software onto School owned devices without the express permission of the IT department.

Users with Internet access may not upload any software licensed to the School or data owned or licensed by the School without explicit authorisation from the member of staff responsible for the software or data.

The School's IT monitoring system records (for each and every user) each web site visit, or e-mail message and each file transfer into and out of its internal networks.

No one should have any expectation of privacy as to his or her Internet usage. The IT department will review internet activity and analyse usage patterns, and may choose to publicise this information to ensure that School internet resources are devoted to maintaining the highest levels of productivity.

Users should not download or view material that is obviously libellous (or otherwise unlawful), or inappropriate in any way, i.e. graphic images, sound files, or music.

Buckswood School reserves the right to inspect any and all files stored on School computing facilities in order to assure compliance with this policy.

The School has in place a firewall to ensure the safety and security of the School's networks. Additional devices may also be installed in the future to further protect these networks. Any user who attempts to disable, defeat or circumvent any School security facility will be subject to disciplinary proceedings. Please see Section 16.

Any files containing sensitive or confidential School information that are transferred in any way across the Internet must be encrypted. Advice and assistance may be sought from the IT department.

A USER WILL BE HELD ACCOUNTABLE FOR ANY BREACHES OF SECURITY OR CONFIDENTIALITY.

Buckswood School’s policy prohibits the sharing of User IDs or passwords obtained for access to Internet sites.

10. Contacting Pupils/Students

If you need to contact pupils/students electronically you should use the school email system - the school system manages an “audit trail” for your protection. Staff should only contact pupils using the school email or the VLE.

Do not respond to invitations from pupils/students in social networking sites. It is expressly forbidden for members of staff to be ‘friends’ (or the equivalent terminology) with pupils/students on social network sites.

Be aware of the professional risks involved in communicating with pupils/students via instant messaging mobile phone, text messaging or other messaging type mediums – though the school recognises that there are situations (for example on school trips, emergencies, or where an immediate response is required) where there is no alternative.

Where possible, staff should use school owned devices to communicate with pupils/students.

11. Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person.

It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated, as part of the PSHE curriculum and in IT curriculum, on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.

Safe and professional behaviour of staff online will be discussed at staff induction.

Personal Social Media

1. School staff WILL NOT invite, accept or communicate with parents and students through any personal social media.
2. If a Student attempts to communicate with a member of staff through any Social Media applications, this must be reported to the Designated Safeguarding Lead.
3. Members of School Staff should set personal social media accounts to the highest levels of privacy settings available.
4. Staff must not publish posts or comments which refer directly or indirectly to matters related to the school and members of its community and must consider the reputation of the school with any posts, in line with contractual duty of contractual obligations.
5. All communication between staff and students should be made through and official school email account or school phone. Staff should not use a personal email account or mobile to make contact unless given prior approval by SMT.

Professional Social Media

All communication and social media content MUST be for the promotion of the school and its students, and accounts must be approved by the PR and Marketing Executive.

All personal details of members of staff MUST NOT be placed on social media.

Social media uploads must be in good taste- never negative to Buckswood, students, staff or other institutions.

Politics, sex and religion MUST NOT be discussed – in line with our internationalism.

Staff must not publish photographs of a child if a parent has opted out of photographic use. If a member of staff is unsure, contact the PR and Marketing Executive (pr@buckswood.co.uk)

Professional Social Media accounts must be registered with an official school email address and the log-in information should be provided to the PR and Marketing Executive (pr@buckswood.co.uk)

Any abusive or inappropriate comments regarding the school must be immediately removed and reported to the PR and Marketing Executive (pr@buckswood.co.uk)

Student Social Media

Students should be aware that third parties such as the media, school and police could access and view their profile and personal information and that inappropriate material found by these third parties could damage the reputation of the school and the student and have a negative impact on future prospects.

Students MUST NOT attempt to make contact with a member of staff through social media, and if a member of STAFF attempts to make contact with them should report it to the DSL.

Students must not post any personal information about themselves or other members of Buckswood staff and student, imagery of the campus or illegal/ distasteful activity whilst in school uniform or within school hours. This could lead to exclusion.

Be aware of copyright and intellectual property rights. Before publishing content, ensure that they have permission of the owner. Infringement could lead to legal action.

The school logo, campus and any intellectual property can only be used on social media with the approval of the school.

Students must not publish content that can represent the school in a negative light, whether this is on a professional or personal social media profile.

The PR and Marketing Executive will regularly review social media postings and any content they do not see as suitable MUST NOT be posted to any social media accounts and must be removed immediately.

Disobeying the guidelines above could result in disciplinary action being taken, which may result in restriction of internet privileges, confiscation of devices and exclusion.

Mobile Phones and Personal Device - for additional information on mobile phone usage by staff, please read the Code of Conduct

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- can make pupils and staff more vulnerable to cyberbullying
- can be used to access inappropriate internet material
- can be a distraction in the classroom
- are valuable items that could be stolen, damaged, or lost can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that all electronic devices are used responsibly in school. Some of these measures are:

- Students are reminded of the school's behaviour policy and various sanctions for breaching the school rules.
- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message

of such content will be disciplined. For more information on the school's disciplinary sanctions read the **school behaviour policy.**

- A member of staff can confiscate mobile phones, and a member of the senior management team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during school lessons or any other formal school activities.
- Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

12. Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.
- Pupils must not take pictures or video recordings of other students or staff with out prior consent, and must not share such images with others

Staff

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils and staff, unless prior consent has been formally recorded. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

More information on this can be found in the **child protection and safeguarding policy**, or in the staff code of conduct

13. Email

All users need to be aware that e-mail carries exactly the same status as other forms of communication, including letters, memos and telephone conversations, and the same consideration and legal implications need to be applied and observed in the use of e-mail as in these other forms of communication.

The definition of Email covers:

i. Electronic Mail services within Buckswood's Local Area Network (internal e-mail).
ii. Electronic Mail sent through the Internet to other organisations/individuals (external e-mail).
iii. The safeguarding of information sent by e-mail.

The School provides an e-mail system to support its academic activities and access to e-mail facilities for all users is granted on this basis. In addition non-pupil users may use these facilities for personal activities including communication and recreational use. However, users are reminded that e-mail sent and received on the School's systems are not private property they remain part of the School's information systems. Personal use should never compromise availability for academic use.

When composing and sending an e-mail, it is expected that the content meets the standards of professionalism which Buckswood School expects of everyone.

It is not permitted to send sexual, racially biased or other inappropriate e-mails, which would infringe the School's code of conduct.

Do not use aggressive, abusive or deliberately anti-social language. Never e-mail hastily or out of anger.

Use of personal e-mail must not detrimentally affect the duties of other email users or disrupt the system, and/or harm the School's image or reputation.

You should not copy or download or forward material that is obviously libellous (or otherwise unlawful), unrelated to work, or inappropriate in any way, i.e. graphic images, sound files, or music.

Access to Internet or web-based e-mail (i.e. Hotmail or Yahoo mail) is permitted, however be aware that this mail is insecure and may present a security threat.

Users are reminded that they are responsible for their own e-mail housekeeping.

Unwanted e-mail should be deleted. If you are unsure how to achieve this, guidelines are available from the IT department.

Those with school email addresses should not give their external e-mail address out carelessly. Only enter it on business circulars and application forms if you are sure that it will not be misused or forwarded on.

Particular attention should be paid to the addressee to ensure the message will reach the intended recipient especially if choosing from an address list of similar names. You should, generally make use of the Global address book for all internal email addresses.

Messages intended for another recipient should be re-directed and then deleted. Any incorrectly addressed messages should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

14. Security

Users should not allow other people to use their network login. Do not leave your PC logged on to the network. As a standard, the School uses a password protected screen saver.

Anti-virus software is installed on every PC connected to the School's network. Anti-virus software must not be disabled or uninstalled for any reason. The anti-virus software is set up to regularly scan each PC for viruses. If you notice that your anti-virus software is not running or scanning, you should immediately report the fact to the Head of IT.

Staff responsible back up their data on school issued equipment.

15. IT Department

It is extremely common for a virus to propagate itself via an e-mail attachment. Commonly the attachment will be an executable file (with .exe, .vbs suffix). If there is any doubt as to the authenticity of an e-mail attachment, it must not be opened; report it to the IT department immediately.

It is also common for a virus to use the Outlook address book to forward itself to others. This means that infected e-mail could be received from a known and trusted source. You should be immediately suspicious if the email is unusual in any way.

Buckswood School maintains the right and ability at any time and without prior notice, where justified, to inspect any information stored on School computing facilities in order to ensure compliance with the policy.

If clarification of any aspects of policy are required, refer to the IT Manager.

16. Use of Technology in Classrooms

This part of the acceptable usage policy has been produced to be read in conjunction with the School's Acceptable Usage Policy (Pupils), the Pupil Behaviour Policy, the Anti-Bullying Policy, and the Child Protection & Safeguarding Policy and Procedures document.

As in all areas of School life, the use of technology for Teaching & Learning purposes should be responsible, respectful and legal.

All technology brought to the classroom (or used for learning in houses or elsewhere on or off the School site) should not cause distraction or disruption either by accident or by design. Devices should only be switched on and accessible when teachers give instructions to that effect.

The School considers inappropriate use of technology in the classroom to be all activity that does not form part of the task as instructed by the teacher. This may include, but is not restricted to the following: gaming, emailing, texting or messaging, taking recordings or photos, using social media, using unsuitable apps and webpages.
Pupils who use technology inappropriately should expect the privilege to be removed and the device to be confiscated for a period of time.

Additional sanctions may be considered in light of any other possible contraventions of related School policies.

17. Confiscation of Technology Protocol

Teachers should aim to ensure that the use of technology in the classroom is managed to be on task and always responsible, respectful and legal. Teachers should feel able to use their discretion as to what constitutes a distraction or disruption to the effective delivery of a lesson and whether it was accidental or intentional.

If it is felt that confiscation of technology is appropriate, then the following protocol should be followed:

1) The teacher asks the pupil/student to switch off the device before handing it in.
2) The teacher checks that the device is switched off.
3) At the earliest opportunity, the teacher brings the device and hands it in personally to the School Office.
4) The device is handed in person to the School Office or placed in a marked envelope and placed in the school safe.
5) Depending on the length of confiscation period, the Principal or Head of Year will contact the pupil's/student's parents to explain that alternative contact methods will be required until the device is returned.
6) The phone will be kept in a secure location during the time that it is confiscated, for the duration of the sanction, in accordance with the school's **behaviour policy**

18. Audio and Visual

In order that staff may understand the guidelines given to pupils/students in respect of Audio Visual devices, the relevant part of the Acceptable Use Policy (Pupils/Students) is reproduced here:

"Recording, filming or take photographs on school premises without permission and with consent of the parent or carer."

"Transmitting any content that is offensive, harassing, or fraudulent."

"Downloading material from the Internet without specific authorisation from the Network Administrator."

"Viewing, sending, or displaying offensive messages or pictures."

"Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts of terrorism, harassment, murder, suicide, or other illegal activity."

19. Consequences of a breach of the Acceptable Use of IT Policy

Unauthorised or inappropriate use of Email and the internet or a failure to adhere to the Acceptable use of IT Policy, will result in disciplinary proceedings being triggered.

If following an investigation it is found that a member of staff has used the school's email or the internet for an unauthorised use or has a failed to adhere to the Acceptable use of IT Policy, this may amount to Unsatisfactory Conduct and the appropriate disciplinary sanctions as set out in the Employee handbook will be applied.

Where it is shown that the Unsatisfactory Conduct has been due to the member of staff's carelessness or that the conduct has had a serious or substantial effect upon the School's operation or reputation, the conduct may be deemed Serious Misconduct and the appropriate disciplinary sanctions as set out in the Employee handbook will be applied.

Please see the employee handbook for further details on what may amount to Gross Misconduct. If upon investigation it is found that a member of staff has committed Gross Misconduct this will lead to the dismissal of that member of staff.

For the avoidance of doubt, where a member of staff has attempted to access inappropriate material, the matter will be referred to the LADO in accordance with the Safeguarding and Child protection Policy.

20. Actions on a breach of the Acceptable Use of IT Policy

If a member of staff breaches the Acceptable use of IT Policy they must report this to the IT Manager as soon as possible, stating when and how they have breached policy and any steps that they have subsequently taken.

For the avoidance of doubt a failure to report a breach of this policy, will amount to Misconduct.

21. Actions on a Smoothwall Notification

If a member of staff is notified by the school's firewall (Smooth wall) that the material they have tried to access using the school's internet, is inappropriate they should take the following steps:

1. Immediately take a screen shot of their screen
2. Email the IT Manager and Safeguarding Officer sending a copy the screen shot, explain what they were accessing and why it was necessary.

If this material is offensive, inappropriate or putting children at risk, the matter will be referred to the LADO in accordance with the Safeguarding and Child Protection Policy and the matter will be investigated as part of the school's disciplinary procedures.

If following an investigation it is found that a member of staff's conduct amounts to amount to Unsatisfactory Conduct the appropriate disciplinary sanctions as set out in the Employee handbook will be applied.

Where it is shown that the Unsatisfactory Conduct has been due to the member of staff's carelessness or that the conduct has had a serious or substantial effect upon the School's operation or reputation, the conduct may be deemed Serious Misconduct and the appropriate disciplinary sanctions as set out in the Employee handbook will be applied.

Please see the employee handbook for further details on what may amount to Gross Misconduct. If upon investigation it is found that a member of staff has committed Gross Misconduct this will lead to the dismissal of that member of staff.