The Phoenix Collegiate

Online Safety Policy

Issued by/responsible person: Raj Kapoor/Rak Mal/Roopinder Shubh	Issue No: 2	Review frequency: every year
Policy number *(to be provided by C. Motard)*: NS12	Approval's date: 20/03/19 by HT, 01/07/19 by Chair of Governors at FGB	Review Date: July 2020
Approval requirement agreed at FGB on 13/11/17: this policy needs to be approved by Head teacher		

Contents

Statement of Intent

At Phoenix Collegiate , we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff. The school is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to prevent any harmful risks.

Legal Framework

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- General Data Protection Regulation
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

This policy will be used in conjunction with the following school policies and procedures:

- Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- General Data Protection Regulation (GDPR) Policy

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities

for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour and Child Protection.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents

within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body, Donovan Williams, has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT and E-Safety Coordinators
- Regular monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors and/or committee(s) meetings.

Headteacher & Senior Leadership Team (SLT)

The Headteacher is responsible for ensuring:

- The safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with e-safety co-ordinator)
- The school's Designated Child Protection Officers should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff, E-Safety Governor and SLT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school.

ICT Network Manager

The ICT Network Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information

- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school's e-safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP before being provided with access to school systems.

Staff & Student Incident Log

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.
There are numerous technologies in place across the school that restricts, monitors and prevents users from breaching the policies in place.
The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					□
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					□
Adult material that potentially breaches the Obscene Publications Act in the UK					□
Criminally racist material in the UK					□
Pornography					□
Promotion of any kind of discrimination				□	
Promotion of racial or religious hatred					□
Threatening behaviour, including promotion of physical violence or mental harm					□
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				□	
Using school systems to run a private business				□	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BMBC and / or the school				□	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				□	

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				□	
Creating or propagating computer viruses or other harmful files				□	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				□	
On-line gaming (educational)		□			
On-line gaming (non-educational)				□	
On-line gambling				□	
On-line shopping / commerce			□		
File sharing			□		
Use of social networking sites			□		
Downloading video broadcasting e.g. Youtube	□				
Uploading to video broadcast e.g. Youtube			□		

Incidents Involving Students

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Student Pastoral Team**	**Refer to police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		□	□	□
Unauthorised use of non-educational sites during lessons	□			□
Unauthorised use of mobile phone/ digital camera/ other handheld device.	□			
Unauthorised use of social networking/ instant messaging/ personal email	□	□		□
Unauthorised downloading or uploading of files		□		□
Allowing others to access school network by sharing username and passwords		□		□
Attempting to access or accessing the school network, using another student's account		□		□
Attempting to access or accessing the school network, using the account of a member of staff		□		□
Corrupting or destroying the data of other users		□		□
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		□		□
Continued infringements of the above, following previous warnings or sanctions		□	Community Police Officer referral	□
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		□		□
Using proxy sites or other means to subvert the school's filtering system		□		□
Accidentally accessing offensive or pornographic material and failing to report the incident		□		□

Incidents Involving Staff

***In event of breaches of policy by the Headteacher, refer to the Chair of Governors.**

Incidents involving members of staff	**Refer to the Headteacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to SLSB LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	□	□	□
Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR	□		□
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	□	□	□
Unauthorised downloading or uploading of files	□	□	□
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	□	□	□
Careless use of personal data e.g. holding or transferring data in an insecure manner	□		□
Deliberate actions to breach data protection or network security rules	□	□	□
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	□	□	□
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	□	□	□
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ students	□	□	□
Actions which could compromise the staff member's professional standing	□		□
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	□		□
Using proxy sites or other means to subvert the school's filtering system	□	□	□
Deliberately accessing or trying to access offensive or pornographic material	□	□	□
Breaching copyright or licensing regulations	□	□	□
Continued infringements of the above, following previous warnings or sanctions	□		□

Education & Training Policy

Education

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities to be provided in the following ways:

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Rules for the use of ICT systems and the Internet are posted in school
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

Digital Literacy

The Department of Education states within the Computing curriculum to support students to become digitally literate whereby, students are able to express themselves and develop ideas through the use of information and communication technology. The school provides a high-quality computing education that equips students to use computational thinking and creativity in the changing world. In particular, student are taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- recognise inappropriate content, contact and conduct and know how to report concerns.

Parent/Carer Education

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school therefore seeks to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, school website, Learning Platform

- Parents / Carers evenings
- High profile events / campaigns eg Safer Internet Day

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Staff Social Media & Communications

Introduction

The internet provides a range of social media tools that allow users to interact with one another; from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter and maintaining pages on internet encyclopaedias such as Wikipedia. These sites are also a fundamental component of communication strategies across Government and business as a means to inform the public and foster openness and engagement with the local community.

While recognising the benefits of Social Media for new opportunities of communication, this policy sets out the principles and standards that staff and the wider school community are expected to follow when using social media, the circumstances in which we will monitor use of social media and the actions we will take in respect of breaches of this policy.

This policy does not apply to Students of Phoenix Collegiate, for whom there is a separate policy.

It is crucial that all stakeholders in The Phoenix Collegiate, including students, parents, staff, partners and the public at large have confidence in the school, and that staff act as ambassadors and advocates. The principles set out in this policy are designed to ensure that the use of social media is responsibly undertaken and that confidentiality of students and staff and the reputation of the school are safeguarded. It is not the intention of Phoenix Collegiate to try to block staff or to impinge on private communications in personal time. However, all members of the school community must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

This policy applies to The Phoenix Collegiate staff and the wider school community. It does not form part of any contract of employment
Under no circumstances may The Phoenix Collegiate logos, crests, typefaces or brands be used or published on any personal web space or on any online or offline medium without prior explicit consent. These are the intellectual property of The Phoenix Collegiate.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.
This policy applies to personal web space such as social networking sites (for example Facebook, Instagram, SnapChat), blogs, microblogs such as Twitter, Chat Rooms, forums, podcasts, open access online encyclopaedias such as Wikipedia and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

Related Policies:

- ICT Policy for Staff
- Staff handbooks, rules and procedures
- E-safety policy
- Child protection and Safeguarding policy
- Anti-bullying policy

The Child protection and Safeguarding policy and Anti-bullying policy can be found on the school website, all others are available at request.

Principles

- Users should be conscious at all times of the need to keep their personal and professional/school lives separate. They should not put themselves in a position where there is a conflict between the school and their personal interests;
- Users should not engage in activities involving social media which might bring The Phoenix Collegiate into disrepute;
- Users should not represent their personal views as those of The Phoenix Collegiate on any social medium;
- Users should not discuss personal information about students, The Phoenix Collegiate and the wider community they interact with on any social media;
- Users should not use social media and the internet in any way to attack, insult, abuse or defame students and/or their family members, colleagues, other professionals, other organisations or The Phoenix Collegiate.

Personal use of Social Media

Staff and members of the wider school community should not identify themselves as members of The Phoenix Collegiate in their personal web-space, unless specifically linked to an approved job role within the school community where it serves a purpose to professionally market the school. This is to prevent information being linked with the school and to safeguard the privacy of staff members, students and parents and the wider school community.

Staff should not have contact through any personal social medium with any student, whether from The Phoenix Collegiate or any other school, other than through those mediums approved by the Senior Leadership Team, unless the students concerned are family members.

If staff and members of the wider school community wish to communicate with students they should do so only through official school sites created for this purpose, which at present are Office 365 and Edmodo.

Information to which staff and members of the wider community have access as part of their involvement with The Phoenix Collegiate, including personal information, should not be discussed on their personal web space. Photographs, videos or any other types of image of students and their families or images depicting staff members, clothing with school logos or images identifying school premises should not be published on personal or public web space without prior permission from the school.

We advise that school email addresses should not be used for setting up personal social media accounts or to communicate through such media. Staff and the wider school community should not edit information about the school on open access online encyclopaedias such as Wikipedia, in a personal capacity.

All staff and members of the wider school community are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Passwords should be kept confidential and changed often, and staff should be careful about what is posted online.

Staff and the wider school community should not post images or videos from school events on any public social media site. Images or videos taken at school events, when such permission has been granted by the school, are for the sole and private use of that individual and their use must be in accordance with the General Data Protection Regulation (GDPR).

This means that images and videos taken at school events should only be posted through the designated person, i.e. compliance officer.

The School accepts that some sites may be used by individual members of staff for professional purposes, to highlight a personal profile with summarised details, e.g. LinkedIn. The School would advise and request that care is taken to maintain an up-to-date profile and a high level of presentation on such sites if The Phoenix Collegiate is listed.

Using Social Media

Communication between students and between students and staff should be via official school sites only for the purposes of an educational context. Edmodo, and Office 365 are the current platforms by which staff and students should communicate and no other medium should be used without careful consideration.

The Headteacher together with senior members of staff at the school, has full responsibility for running the school's official website. Only members of SLT or those staff who have received specific and explicit authority from the Headteacher, are permitted to post material on any social media site in the name of, or on behalf of, The Phoenix Collegiate. No other social media platforms may be set up by any member of the school community which have a direct or indirect connection with The Phoenix Collegiate.

All interaction with social media sites should be done with responsibility and respect.

Friends/Befriending:

• One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. **The School prohibits staff from accepting invitations to "friend" students, or students' family members/friends.**

• **Staff must not initiate friendships with students, or students' family members/friends, under any circumstances.**

Staff should exercise caution in accepting or initiating friendships with former students. The School's view is that such friendships are appropriate only when former students are of an age whereby the relationship can be considered as being between equals not that of a teacher/student or adult/child i.e. after several years have elapsed.

• Staff who maintain social networking friendships with work colleagues, are required to adhere to the requirements below relating to content of interactions.

Content of interactions:

- Staff must not make reference on social networking sites to the School, its employees, students, and their families. If staff adhere to this recommendation then the personal content of an individual's social networking memberships is unlikely to be of concern to the School. However, if employment at the School is referred to, then the information posted would need to comply with the conditions set out below.

- Any references made to the School, its employees, students and their families should comply with the School's policies on conduct/misconduct, equal opportunities, and bullying and harassment.

- Staff must not post information on a social networking site which is confidential to the School, its employees, its students or their families.

- Staff must not post entries on social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the School into disrepute.

- Staff should not use the School logo on their own personal social networking accounts, and should not post any photographic images that include students or members of staff.

- Staff must not download copyrighted or confidential information. If this is done accidentally or in error, staff should notify their line manager as soon as possible.

- Staff must not express personal views which could be misinterpreted as those of the School.

- Staff must not commit the school to purchasing/acquiring goods/services without proper authorisation.

- When posting information on a social networking site, staff must not post any entry that puts their effectiveness to perform their normal duties at risk.

- If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the School, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Staff should discuss any concerns with their head teacher/line manager in the first instance.

Communication

Email

- Digital communications with students (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in child protection policy).

- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);

- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal e-mail addresses.

- School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ students.

Mobile Phones

- **School** mobile phones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.

- **Staff** should not be using personal mobile phones in school during working hours when in contact with children.

- Students should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list is published to all staff on a termly basis, but can also be obtained from the data office or the child protection officers in school.

- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher or the ICT network manager.

- Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website which is used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Any removable media used in school which contain sensitive/confidential information will need to be encrypted.

- Any removable media used in school will be checked by the Anti-Virus to make sure it is safe before use.

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

- Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

- Staff using removable media to store confidential data need to adhere to the GDPR Policy.

Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Staff will preview any recommended sites before use.

- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.

- **All** users must observe copyright of materials published on the Internet.

- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.

- The school only allows the E-Safety Co-ordinator, ICT co-ordinator and SLT to access to Internet logs.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults					**Students and young people**			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		□								□
Mobile phones used in lessons					□					□
Use of mobile phones in social time		□								□
Taking photographs on mobile devices					□					□
Use of PDAs and other educational mobile devices		□					□			
Use of school email for personal emails					□					□
Social use of chat rooms/facilities					□					□
Use of social network sites				□					□	
Use of educational blogs		□					□			

Guidance is also available from Human Resources

Security

Members of Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.
In using social networking sites, members of staff are recommended to post only content that they would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the School as their employer.
Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them. Accessing of, or reference to, such personal information by students and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to their line manager in the first instance.
If a member of staff becomes aware that a student (or group of students) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they must report this to the Head teacher so that the appropriate process can be followed.

Policy breaches

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy & Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal where the breach is considered to constitute gross misconduct.

Information shared through social networking sites, even on private spaces, is subject to Copyright, Data Protection, Freedom of Information, Equality, Safeguarding and other legislation.

Where staff work in roles that are governed by professional bodies/professional codes of conduct, the professional rules relating to social networking applied to them may be more stringent that those within this Policy.

Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of The Phoenix Collegiate or any illegal acts/acts that render The Phoenix Collegiate liable to third parties, may result in legal action, disciplinary action or sanctions in line with the published School policies.

Monitoring of Internet Use

School computers and any data held on them are the property of Phoenix Collegiate. The School may monitor usage of its internet, online content, online services and email services at any time, without prior notification or authorisation from users, in order to ensure compliance with statutory, regulatory and internal policy requirements.
Use of the internet is monitored by automated tools to ensure compliance with the School's Acceptable Use policy and to prepare generic trend and usage statistics associated with internet use. This information may be used for the purposes of disciplinary proceedings where breaches of policy are identified.

Guidelines for safe Social Media usage can be found on the following websites:

http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks http://www.childline.org.uk/explore/onlinesafety/pages/socialnetworking.aspx

http://www.getsafeonline.org/social-networking/social-networking-sites/#.Uq7_0lPs084
http://www.bbc.co.uk/webwise/courses/social-media-basics/lessons/stay-safe-on-social-networks

Cyberbullying

Phoenix Collegiate takes the issue of Cyberbullying extremely seriously and we will review our School policy in this regard annually, in response to on-going rapid developments in technology and social media.

Government guidance on the prevention of Cyberbullying can be found online at:
https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00239-2008

If any member of staff is subjected to Cyberbullying, or inappropriate or threatening comments via social media they should not respond or retaliate but should report this immediately to the Associate Head teacher who will decide on action to be taken accordingly, including involving the Police if necessary.

Staff & Student Acceptable Use Policy

Acceptable Usage Policy

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules.

- **Staff and regular visitors** to the school have an AUP that they must read through and sign to indicate understanding of the rules.

The computer systems within school are made available to students, staff and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The school's Acceptable Use Policies have been drawn up to protect all parties – the students, the staff, other adults and the school and are reviewed on a regular basis.

Staff and other adults wishing to use the schools computer systems, email or Internet should sign a copy of this Acceptable Use statement below and return it to the Head teacher for approval.

- All Internet activity should be appropriate to staff professional activity or the student's education.

- Access should only be made via the authorised account and password, which must not be made available to any other person.

- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden.

- Users making threats or offensive comments via e-mail, chat, School VLE or social media will be dealt with accordingly.

- Users are responsible for all e-mail sent and for contacts made that may result in email being received

- Use for personal financial gain, gambling, political purposes or advertising is forbidden

- Copyright of materials must be respected

- Posting anonymous messages and forwarding chain letters is forbidden

- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media

- Appropriate use of Machines and Mobile Technologies (any damage or vandalism will result in the user been banned for future use)

- Copyright of materials must be respected

- Posting anonymous messages and forwarding chain letters is forbidden

- Users should not engage in activities involving social media which might bring The Phoenix Collegiate into disrepute;

- Users should not represent their personal views as those of The Phoenix Collegiate on any social medium;

- Users should not discuss personal information about students, The Phoenix Collegiate and the wider community they interact with on any social media;

- Users should not use social media and the internet in any way to attack, insult, abuse or defame students and/or their family members, colleagues, other professionals, other organisations or The Phoenix Collegiate.

- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

- If you access any site on the internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the pro-forma to the identified member of staff.

- Use of social networking sites for leisure use is forbidden.

Misuse of schools computer equipment, Mobile Technologies/Tablets, email or the Internet are serious offences. Phoenix Collegiate has an obligation to monitor the use of the e-mail and Internet services provided. This information may be recorded and may be used in disciplinary procedures if necessary. Phoenix Collegiate reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

AUP Policies for Staff, Students, Parents/Carers and Visitors have been amended accordingly to cater for the differential use of each group. There are policies in place to make sure all users who access the schools network have signed the appropriate AUP before they are allowed access to it. (copies of these are included at the end of the document).

Monitoring & Reporting Policy

Monitoring

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider (wave9). Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Student Pastoral Managers, Achievement Coordinators, staff or members of the Senior Leadership Team depending on the severity of the incident.

- E-Safety Coordinator and ICT Network manager will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems

- Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. This is part of the school safeguarding protocol. (If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Headteacher).

Incident Reporting

- Users understand how to report abuse and concerns through a range of mechanisms. Students report abuse through using the 'Report It' from the school website or through the use of Tootoot off Office 365. In student planners, a list of useful numbers are highlighted to report abuse such as CEOP and Childline. Assemblies and Computing lessons regularly highlight how to report abuse and concerns through the mechanisms described.

- Staff understand the any e-safety incidents must immediately be reported to the Headteacher who will investigate further following e-safety and safeguarding policies and guidance.

- Parents/carers are regularly updated with how to report incidents through the eParent Mail newsletters, school website CEOP weblinks, Student/Parent Acceptable Use Agreement and through the Parents section of the school website.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Below are the responses that will be made to any apparent or actual incidents of misuse.

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					
Promotion or conduct of illegal acts, eg under the child protection, obscenity,					

computer misuse and fraud legislation					
Adult material that potentially breaches the Obscene Publications Act in the UK					□
Criminally racist material in the UK					□
Pornography					□
Promotion of any kind of discrimination				□	
Promotion of racial or religious hatred					□
Threatening behaviour, including promotion of physical violence or mental harm					□
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				□	
Using school systems to run a private business				□	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BMBC and / or the school				□	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				□	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				□	
Creating or propagating computer viruses or other harmful files				□	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				□	
On-line gaming (educational)		□			
On-line gaming (non-educational)				□	
On-line gambling				□	
On-line shopping / commerce			□		
File sharing			□		
Use of social networking sites			□		
Downloading video broadcasting e.g. Youtube	□				
Uploading to video broadcast e.g. Youtube			□		

If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally

racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse.

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows

Note: The school will become actively involved in any incidents which have occurred outside of school which has any impact on the school, its students or staff.

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Student Pastoral Team**	**Refer to police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		□	□	□
Unauthorised use of non-educational sites during lessons	□			□
Unauthorised use of mobile phone/ digital camera/ other handheld device.	□			
Unauthorised use of social networking/ instant messaging/ personal email	□	□		□
Unauthorised downloading or uploading of files		□		□
Allowing others to access school network by sharing username and passwords		□		□
Attempting to access or accessing the school network, using another student's account		□		□
Attempting to access or accessing the school network, using the account of a member of staff		□		□
Corrupting or destroying the data of other users		□		□
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		□		□
Continued infringements of the above, following previous warnings or sanctions		□	Community Police Officer referral	□

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		□		□
Using proxy sites or other means to subvert the school's filtering system		□		□
Accidentally accessing offensive or pornographic material and failing to report the incident		□		□

For Staff

Incidents involving members of staff	**Refer to the Headteacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**Referral to SLSB LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	□	□	□
Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR	□		□
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	□	□	□
Unauthorised downloading or uploading of files	□	□	□
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	□	□	□
Careless use of personal data e.g. holding or transferring data in an insecure manner	□		□
Deliberate actions to breach data protection or network security rules	□	□	□
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	□	□	□
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	□	□	□
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ students	□	□	□
Actions which could compromise the staff member's professional standing	□		□
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	□		□
Using proxy sites or other means to subvert the school's filtering system	□	□	□
Deliberately accessing or trying to access offensive or pornographic material	□	□	□
Breaching copyright or licensing regulations	□	□	□
Continued infringements of the above, following previous warnings or sanctions	□		□

Introduction

Phoenix Collegiate collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Purpose of our policy

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the new GDPR, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

General Data Protection Regulation Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Employee responsibilities

All employees are responsible for:

- Checking that any personal data that they provide to the school is accurate and up to date.
- Informing the school of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the school may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees collect information about other people (e.g. personal circumstances, or about employees), they must comply with the GDPR Policy.

Physical Security & Personal devices

Physical security applies to our buildings, storage systems and removable media. Therefore the school will:

- Ensure paper documents are kept in locked cupboards of filing cabinets

- Never leave printed personal information on desk, tables or notice boards
- Keep portable electronic devices secure both on/off school premises

Electronic devices

- Ensure our staff choose strong passwords
- Ensure personal devices and removable media have levels of encryption
- To always delete/destroy appropriate information if device is no longer needed
- Ensure our staff are vigilant when transporting electronic devices (especially smaller devices)

Data security, disposal & Sharing Personal data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
- What personal information is allowed to be shared and whom they can share it…includes; Health authorities, local government, other schools, Educational bodies, Social services & Integrated services (Troubled families)
- To use our Paper confidential waste bags when destroying data on paper
- To use the Data manager when transferring data externally (via web-x, S2S systems)
- To use internal secure resources when transferring internally (Resources/staff share)
- In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may readily see that data
- Multiple logins can occur at any terminal, staff must ensure they log off or lock out when leaving that terminal

Internet, websites & Third party processing

The Phoenix Collegiate is aware that our data processed by another handler still makes us responsible for data processing done by a third party. Therefore the school will make sure:

- Written agreements with third party processors covering security are in place
- Ensure that third party processors only act on our instruction
- To ensure staff ask permission before publishing data/photos online

- To ensure Restrictive access is applied to online resources using usernames/passwords

- To ensure staff are aware that metadata/cookies attract its own specific regulations

School Specific Data Collection

The school will always seek consent/parental and carer consent for the following:

- Photographs/ recordings of students used in school publications, including those to be used in local newspaper/ newsletters.

- Photographs/ recordings of students that are used internally by the school, for school projects

- Photograph/ recordings of students, staff & parents to be used on the website.

- To include the following consent forms in our data collection packs:- Privacy policy notice, Biometrics form, Connexions , media form & Acceptable user policy

Retention of data

The school will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary.

Data control, Audits & Recovery

The school undertakes regular audits every term to identify correct and fair processing of personal and sensitive data. We provide our local authority/government with:

- A Student Census, provided every term covering student information plus additional fields are included depending on which Census is required

- Workforce Census

- Finance audits for bursary funding

Our Data in school, including cloud services are provided with recovery and back-up systems dedicated to restore lost or corrupt data within the network. Regular back-up servers use a redundant array of independent disks and are scheduled to capture a snapshot of data on a daily basis.

Firewall configuration

Where Electronic Equipment is used to capture, process and store data on the network, Firewall is installed, configured and maintained for threats against school data. Website filtering is applied for malicious and inappropriate content along with antivirus and malware checking.

CCTV

Capturing images of identifiable people means GDPR principles apply to CCTV and subject access requests can be made. At Phoenix signs indicating CCTV is in operation are in place to make staff, students & visitors aware CCTV is being used. CCTV footage is only kept for a set period and only used where appropriate.

Requests for the disclosure of personal data

Requests from the Police, Government bodies or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

Subject access request & Complaints

Phoenix Collegiate procedures for responding to subject access requests made under the GDPR.

Rights of access to information

All individuals who are the subject of personal data held by the school are entitled to:
• Ask what information the school holds about them and why.
• Ask how to gain access to it.
• Be informed how to keep it up to date.
• Be informed what the school is doing to comply with its obligations under the GDPR.

These procedures relate to subject access requests made under the GDPR.

Subject access requests (SARs)

- Individuals have the right to obtain confirmation that their data is being processed.

- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
-
- The school will verify the identity of the person making the request before any information is supplied.

- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

- All fees will be based on the administrative cost of providing the information.

- All requests will be responded to without delay and at the latest, within one month of receipt.
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details are provided below.

Status of the policy

This policy has been approved by the Governors and any breach will be taken seriously and may result in formal action.

Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Headteacher.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact a data controller who will also act as the contact point for any subject access requests. Mike Smith - Headteacher, Don Williams - Governor or the Data Manager.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

Review

This policy will be reviewed annually and updated as necessary to reflect best practice or amendments made to relevant legislation. The policy review will be undertaken by the Head teacher, Staff & Governors.

Technical Security

Technical Security

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It ensures that the relevant people receive guidance and training and will be effective in carrying out their responsibilities.

- The school's technical systems manage ways to ensure that the school meets recommended technical requirements.
- Regular reviews and audits of the safety and security of school technical systems are updated
- Devices are kept up to date with the latest security patches, up to date anti-virus and firewalls to protect the system.
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- Monitoring software is in place that can track any misuse online or on devices.

Password Security

A safe and secure username / password system is essential and is applied to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 4 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

- Should only let school staff know their in-school passwords if requested to do so.
- Inform staff immediately if passwords are traced or forgotten. All ICT staff are able to access the network to allow students to change passwords.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or ICT Network manager.
- Students should not bring in their own equipment unless asked to do so by a member of staff.

Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted. This is linked with the GDPR Policy.
- All should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The responsibility for the management of the school's filtering is held by the Network Manager.

They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- **be logged in change control logs**
- **be reported to a second responsible person** (Head of ICT):

All users have a responsibility to report immediately to the Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists.

Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider 'Wave9'

- The school has provided enhanced / differentiated user-level filtering through the use of the (Wave9 Sophos) filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / students / students etc.)

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher or E-Safety Officer.

- Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems

- Any filtering issues should be reported immediately to the filtering provider.

- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (Network Manager and also checked off by the Headmaster). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school therefore monitors the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring takes place by using AB Tutor which is installed on all ICT teacher PC'S that lets the teacher monitor what students are doing and it is also checked by the ICT Support staff and any issues reported.*

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: -

- Network Manager and SLT
- Online Safety Group
- Online Safety Governor / Governors committee
- Wave 9 / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision

ICT STANDARDS
For Staff and Students

The computer systems within school are made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete files that may be held on its computer systems or to monitor any Internet site visited.

- All Internet activity should be appropriate to staff professional activity or the student's education
- Access should only be made via the authorised account and password, which must not be made available to any other person
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden
- Users making threats or offensive comments via e-mail, chat, learning gateway or social media will be dealt with accordingly.
- Users are responsible for all e-mail sent and for contacts made that may result in email being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- Appropriate use of Machines and Mobile Technologies (any damage or vandalism will result in the student been banned for future use)

Acceptable Use Statement

Student

The School's Acceptable Use Policies have been drawn up to protect all parties – the students, the staff, other adults when using the school computer systems. These policies are reviewed on a regular basis and are amended accordingly to cater for the differential use of each group.

Students wishing to use the schools computer systems, email or Internet should sign a copy of this Acceptable Use statement and return it to the school for the Head teacher to approve.

- All Internet activity should be appropriate to the student's education
- Access should only be made via the authorised account and password, which must not be made available to any other person
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- Any physical damage caused to ICT equipment will result in the person replacing the equipment.
- If you access any site on the internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the pro-forma to the identified member of staff.
- Use of social networking sites for leisure use is forbidden.

Misuse of schools computer equipment, Mobile Technologies/Tablets, email or the Internet are serious offences. Phoenix Collegiate has an obligation to monitor the use of the e-mail and Internet services provided. This information may be recorded and may be used in disciplinary procedures if necessary. Phoenix Collegiate reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

Internet and Electronic Mail Policy for Students

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, websites and bulletin boards whilst exchanging messages with Internet users throughout the world. Staff will provide guidance to students as they make use of the Internet to conduct research or other studies related to the curriculum. Whilst Phoenix Collegiate uses filters to attempt to exercise considerable control of the material available, parents are advised that it is still possible to access and create material which is potentially offensive or undesirable. It is for this reason that all students must obtain parental permission and sign the attached ***User Agreement and Parent Permission Form*** and return it to their form tutor at school. A copy of the ***Acceptable Use Statement*** is provided for parents' information. Students and parents/guardians should be aware that usage of all machines and Tablets in school can be, and is, closely monitored by our technical staff.

USER AGREEMENT AND PARENT PERMISSION FORM

Name of Student: _____ **Form:** _____

I have read and accept the conditions of the ***Acceptable Use Statement.*** I am aware that breaking these conditions may result in a loss of access to the internet in school as well as other disciplinary action.

Student's Signature: _____

As parent/carer of the above student I grant my permission for my child to access networked computer services such as electronic mail and the Internet, and that I will support the school in enforcing its ***Acceptable Use Statement.***
I recognise that violations may result in a loss of access as well as other disciplinary action.

Parent/Carer's Signature: _____

Acceptable Use Statement

Staff

The computer systems within school are made available to students, staff and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The school's Acceptable Use Policies have been drawn up to protect all parties – the students, the staff, other adults and the school and are reviewed on a regular basis.

Staff and other adults wishing to use the schools computer systems, email or Internet should sign a copy of this Acceptable Use statement and return it to the Head teacher for approval

- All Internet activity should be appropriate to the staff member teaching and learning
- Access should only be made via the authorised account and password, which must not be made available to any other person
- Users should be conscious at all times of the need to keep their personal and professional/school lives separate. They should not put themselves in a position where there is a conflict between the school and their personal interests;
- Users should not engage in activities involving social media which might bring The Phoenix Collegiate into disrepute;
- Users should not represent their personal views as those of The Phoenix Collegiate on any social medium;
- Users should not discuss personal information about students, The Phoenix Collegiate and the wider community they interact with on any social media;
- Users should not use social media and the internet in any way to attack, insult, abuse or defame students and/or their family members, colleagues, other professionals, other organisations or The Phoenix Collegiate.
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Data Protection and Copyright of materials must be respected and encrypted devices used for transferring confidential data

- Posting anonymous messages and forwarding chain letters is forbidden

- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media

- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

- If you access any site on the internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the pro-forma to the identified member of staff.

- Use of social networking sites for leisure use is forbidden.

Misuse of schools computer equipment, Mobile Technologies/Tablets, email or the Internet are serious offences. Phoenix Collegiate has an obligation to monitor the use of the e-mail and Internet services provided. This information may be recorded and may be used in disciplinary procedures if necessary. Phoenix Collegiate reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

ACCEPTABLE USE AGREEMENT

Name of Staff Member: _____

I have read the statement above and agree to abide by the conditions. I understand that misuse of schools computer systems, email or the internet are serious offences and could lead to disciplinary procedures, up to and including dismissal

Staff Member Signature: _____

Date: _____

Visitor User Acceptable Use Statement

Community and Visitor Users

The computer systems within school are also made available to visitors should they need to use it. The school's Acceptable Use Policies have been drawn up to protect all parties – the students, staff and visitors. The policy is reviewed regularly to keep up do date with the changing online environment.

Visitors and other adults wishing to use the schools computer systems, email or Internet should sign a copy of this Acceptable Use statement which will be returned to the Head teacher for approval.

- All Internet activity should be appropriate to the student's education
- Access should only be made via the authorised account and password, which must not be made available to any other person
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applies as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- If you access any site on the internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the pro-forma to the identified member of staff.

Misuses of schools computer equipment including Mobile Technologies/Tablets, email or the Internet are serious offences. Phoenix Collegiate has an obligation to monitor the use of the e-mail and Internet services provided. This information may be recorded and may be used in disciplinary procedures if necessary. Phoenix Collegiate reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

ACCEPTABLE USE AGREEMENT

Name of Staff Member: _____

I have read the statement above and agree to abide by the conditions. I understand that misuse of schools computer systems, email or the internet are serious offences and could lead to disciplinary procedures, up to and including dismissal

Staff Member Signature: _____

Date: _____

The Phoenix Collegiate
STAFF
Home Device Policy

At Phoenix Collegiate, we understand that school-owned electronic devices are used by members of staff outside of the school. The school has an efficient and practical approach which acknowledges the use of devices and with this in mind, this policy is intended to ensure that:

- Members of staff are responsible users, and remain safe while using the device.
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.

Electronic devices can enhance work and learning opportunities, and enable people to be creative. In return, members of staff need to agree to be responsible users by understanding the following:

1. The school monitors the use of all ICT systems and electronic devices.
2. All school-owned devices allow access to the school network off-site. In the event of a breach of security or data, devices will be removed and disciplinary action will be taken.
3. Members of staff only use school-owned electronic devices for educational purposes.
4. Usernames and passwords are not disclosed to others.
5. Ensure that the guidelines set out in the GDPR and Online Safety Policy are followed when connecting the device to any networks or wireless internets.
6. Members of staff are not permitted to install or remove software from a school-owned electronic device.
7. The school and ICT department may ask for the device back at any time to apply security patches and updates.
8. It is the schools responsibility to investigate and repair any technical issues with the device, members of staff are not permitted to send the device to any third parties.
9. If a school-owned electronic device is damaged or lost outside of school hours or off-site, the member of staff at fault may be responsible for paying damages.

<u>Think about Positive Use of the Internet</u>

At Phoenix we understand that using the internet is important when raising educational standards and enhancing teaching and learning.

However, when accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. We aim to ensure that our users are

protected and educated to ensure that they are aware of these risks and practice using the internet safely.

Staff Declaration Form

All members of staff are required to sign this form before they are permitted to use electronic devices that are owned by the school.
I have read The Phoenix Collegiate STAFF Home Device Policy and understand that:

- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the Headteacher.
- Illegal, inappropriate or unacceptable use of school equipment will result in disciplinary action.
- The school reserves the right to monitor my emails, phone calls, internet activity and document production.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

Staff Member Sign and Print	
Date:	
ICT Systems Manager Sign and Print	
Date:	

The Phoenix Collegiate
STAFF
Email Etiquette

Before using e-mail to communicate, it is important to be aware of the etiquette of electronic communication. The following tips and hints are intended as aids to promote the appropriate and effective use of e-mail.

1. Keep messages brief and to the point.
2. Consider using the telephone or a face-to-face meeting for handling sensitive, difficult, complex, or emotional issues
3. Let senders know if you are receiving emails you need. For example replies to include:
    - Keep sending this sort of critical information.
    - Send this sort of information to [name] on my team, not me.
    - Please don't send me this kind of information
4. Keep the content professional and write with the same respectful tone you use in verbal communications.
5. Be careful with humour and sarcasm; the reader cannot hear the tone of your voice nor see the expression on your face, if you must use☺.
6. State the subject of the message clearly
7. Put the action required of the receiver on the Subject line
8. Put "FYI" (For Your Information) at beginning of the Subject line if the message is simply to inform the receiver, no answer is required, and there is no urgency for reading
9. For very short messages, consider putting the message on the Subject line with two asterisks in front and two in back. E.g. **Curriculum meeting Today at 13:00 is cancelled**
10. Ensure that you send your email to the person from whom you would like a response. C.c. other colleagues that you wish to inform but do not require a response from.
11. Limit copies (cc) to those who are involved and really need to know but who do not need to respond.
12. Use the option **"Reply All"** sparingly and only when there is a need to inform everyone that received the original message.
13. Use "High" priority sparingly. Use this when the message or a response is time sensitive.

14. Manage your mailbox. Provide timely responses.

15. Do not forward any chain letter – it is unsolicited mass e-mail, otherwise known as "spam". It is prohibited by school policy

16. Follow Phoenix Collegiate's AUP