E-Safety Policy (incorporating Mobile Technology and Acceptable Use)

Independent Day School for Boys and Girls (Whole School including EYFS)

Our Lady of Sion School

Next review: October 2019

E-SAFETY POLICY (incorporating Mobile Technology and Acceptable Use)

1. Introduction
2. Roles and responsibility
3. Communicating School policy
4. Making use of ICT and the internet in School
5. Learning to evaluate internet content
6. Managing information systems
7. Emails (See Appendix 2 Email protocol)
8. Policy and guidance of safe use of children's photographs and work
9. Social networking, social media and personal publishing
10. Mobile phones and personal devices
11. Sexting
12. Managing emerging technologies
13. Sanctions
14. Monitoring and review

Appendix 1 Internet protocol
Appendix 2 Email protocol
Appendix 3 – Mobile Devices Acceptable Use Policy

1. Introduction

This policy applies to staff and pupils at the school and links with our Safeguarding and Anti-bullying policies.

The School recognises that ICT and the internet are important 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.

E-safety covers the internet but it also covers mobile phones/devices, iPads and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. 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 e-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 be an aid in regulating 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. E-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 policy and procedures.

2. Roles and responsibility

The Headmaster and Governors will ensure that the E-safety policy is implemented and compliance with the policy monitored but the day-to-day management of E-safety in the School is the responsibility of the Deputy Headmaster. They will work closely with other members of the Senior Leadership Team and academic staff in this regard. Staff must always

report inappropriate use of the internet to the Designated Safeguarding Lead who will take appropriate action.

3. Communicating School policy

This policy is available on the School's intranet for parents, staff, and students to access when and as they wish.

E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, as well as being specifically addressed in the PSHEE curriculum. E – safety posters are displayed in key areas.

Pupils should comply with the following protocols as well as complying with the rules about security set out in this policy:

(a) internet protocol (Appendix 1);
(b) e-mail protocol (Appendix 2);
(c) mobile devices acceptable use (Appendix 3)

Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Pupils witnessing misuse by other pupils should talk to a member of staff about it as soon as possible.

4. Making use of ICT and the internet in School

Using ICT and the internet in School brings many benefits to pupils, staff and parents. The internet is used in School to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer or device connected to the school network. The School cannot accept liability for the material accessed, or any consequences of internet access.

Expectations of use of School computers apply to staff and pupils both in and out of lessons. See also Appendix 1 - Internet protocol.

5. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum.

Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate;

- To acknowledge the source of information used and to respect copyright.

If staff or pupils discover unsuitable sites then the URL, time, date and content must be

reported to the IT Department. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the IT Department or a member of the Senior Leadership Team. Regular checks will take place to ensure that filtering services are working effectively.

6. Managing information systems

The School is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of School data and personal protection of our School community very seriously. This means protecting the School network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT Support team, led by the Network Systems Manager and virus protection software will be updated regularly. Some safeguards that the School takes to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any School computers. Files held on the School network will be regularly checked for viruses;
- The use of user logins and passwords to access the School network will be enforced. Passwords must be kept confidential and changed immediately if it is believed someone else knows it.
- Computers should be logged off or locked if the workstation is left for any period of time.
- The School has a firewall in place to ensure the safety and security of the School's networks and additional devices may be installed in the future to further protect these networks. Pupils must not attempt to disable, defeat or circumvent any of the School's security facilities.
- Attempting to obtain (or attempt to obtain) unauthorised access to any part of the School's computer system, or any information contained on the system will be treated as a serious breach of School discipline.
- Anti-virus software is installed on every PC connected to the School's network. Pupils must ensure this is running at all times and report any problems to the IT department immediately. Users of the School's facilities should be aware of the potential damage that can be caused by computer viruses and the following rules apply:
    - (a) anti-virus software must not be disabled or uninstalled for any reason;
    - (b) any pupil believing he / she has received a message that includes a virus must not open it and report it to the Network Systems Manager, Junior School Senior Teacher or Deputy Head immediately;

Pupils who are concerned about any aspect of the safety and security of the School's networks should speak to Network Systems Manager, Junior School Senior Teacher or Deputy Head. The Network Systems Manager monitors the internet activity and informs the Deputy Headmaster and Junior School Senior Teachers (if appropriate) of any inappropriate use.

7. Emails (See Appendix 2 Email protocol)

The School uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Access in School to external personal email accounts may be blocked. The School has the right to monitor emails and their contents but will only do so if there is suspicion of inappropriate use.

Staff should be aware of the following when using email in School:

- Staff should only use official School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.

- Emails sent from School accounts should be professionally and carefully written. Staff

are representing the School at all times and should take this into account when entering into any email communications.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their line manager or a senior member of staff.

- Staff must tell their manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted in School.

Students should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- All pupils are provided with a School email account and pupils may only use approved email accounts on the School system.

- Pupils should not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases will be restricted.

- Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

8. Policy and guidance of safe use of children's photographs and work

Photographs and pupils' work bring our School to life, showcase our students' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. (As per parental contract).

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the School will be used in public and children may not be approached or photographed while in School or doing School activities without the School's permission.

The School follows general rules on the use of photographs of individual children:

Consent from parents will cover the use of images in:
- Use in the school's promotional material such as the prospectus, the website or social media
- Press and media purposes
- Educational purposes as part of the curriculum or extra-curricula activities.

Unpublished electronic and paper images will be stored securely.

Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities, which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
For public documents, including in newspapers, full names will not be published alongside images of the child without the written permission from parents. Groups may be referred to collectively by year group or form name.

Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

Only official school cameras may be used to take images.

9. Social networking, social media and personal publishing

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 students so that they can make their own informed decisions and take responsibility for their conduct online. The School will normally block/filter access to social networking sites via the School network.

Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught in PSHEE 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 on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of the intranet (Appendix 1- Internet protocol).

- Any social media sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Official School blogs created by staff or students/year groups/School clubs as part of the School curriculum 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.

- Guidance for the safe and professional behaviour of staff online is provided through the staff code of conduct and Safeguarding Policy.

10. Mobile phones and personal devices

Staff personal mobile devices must never be used to take photographs or record students either in school or off-site including in the EYFS setting. Staff should never use their personal mobile phone to contact students. School equipment must always be used for these circumstances. 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.

Mobile phone and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these 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 that:

- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.
- Many mobile phones are able to access 3G and 4G networks which enable pupils to bypass the school's web filtering system.

We acknowledge that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently.

We also recognise the importance of the technologies present in modern mobile phones such as internet access, cameras and MP3 playback and may wish to utilise these functions to support teaching and learning in a controlled environment.

In order to safeguard our pupils throughout the school day the following acceptable use procedures are in place.

Students in the Junior School are not permitted to bring mobile devices into school. If any mobile phones are brought into school they should be handed to the office for safe keeping until the end of the school day.

Students in the Senior School are permitted to bring mobile devices into school but by doing so; they agree to abide by our acceptable use rules set out in Appendix 3.

Parents are not allowed to use their mobile devices within the EYFS setting and there are notices informing visitors of this on all the entry points.

11. Sexting

Anti-sexting also forms part of the Safeguarding Policy and is a form of peer on peer abuse. The term 'sexting' is a derivation of 'texting' but relates to the sending of indecent images, videos and/or written messages with sexually explicit content. These are created and sent via electronic communication devices such as mobile telephones, tablets, laptops and desktop computers. They are often 'shared' via social networking sites and instant messaging services.

Our Lady of Sion School will not tolerate sexting, it is inappropriate and illegal amongst young people and can have extremely damaging and long-lasting consequences. When the school is aware that sexting has taken place the DSL will treat this as a child protection matter and follow the Safeguarding Policy. The DSL will contact the Police Liaison Officer and/or the MASH for advice and possible support. This is also referred to in our Anti-bullying policy.

Legal Implications for pupils

Sexting potentially breaches several civil laws concerned with the creation, possession and distribution of child pornography and indecent images. These are images which show partial (where breasts or genitals are exposed) or full nudity and/or feature sexual acts being performed. It is illegal for student to make and/or share images such as these, even if they are images of themselves, which have been taken personally or with consent. Students who engage in sexting (to any extent) are at risk of receiving a police caution and/or being placed on a register for sexual offenders for a period of several years (which can have serious ramifications in adulthood with regards to employment, travel etc). Sexting can also (in some cases) be viewed as a crime under the Malicious Communications Act.

The misuse of IT, such as sexting, inappropriate comments on Facebook, being the object of cyber-bullying and online grooming are all potential welfare concerns and identified as such in our Safeguarding Policy.

As staff, we have a responsibility to work with parents and carers in ensuring that all pupils are fully aware of the dangers and possible repercussions of sexting. In school, this information will be communicated to pupils during PSHE lessons, in assemblies and through parental talks.

Sexting incidents are often complicated as they potentially involve a large number of pupils and those involved could be victims or perpetrators or both.

If an incident of sexting is reported or suspected:

- If “sexting” is reported by the victim or deemed to be a safeguarding matter, then it must be treated as a disclosure of a safeguarding matter and referred to the Designated Safeguarding Lead who will report the incident to the MASH.
- If deemed to be a disciplinary issue or a potential crime, it must be reported to the Headmaster. Parents and carers will be notified and the incident will be reported to the local MASH team or the police, as appropriate.
- Pupils will be sanctioned in accordance with our Behaviour Policy. Sexting is a serious offence and dependent on motive, intent, pressure or coercion, those involved may be issued with fixed term or, in extreme cases, even permanent exclusion.
- Pupils may also be subject to interview by the Police and confiscation of their electronic devices.

Guidance for staff if you suspect that an offence has been committed:

- If you suspect that “sexting” has taken place or you become aware of indecent images circulating in school or a pupil refers an incident of “sexting” to you, then you must refer it straight away to the Headmaster or Designated Safeguarding Lead.
- You are not permitted to forward, copy or print any sexting images and may inadvertently implicate yourselves simply by viewing such material.
- If you are in any doubt whatsoever, seek immediate advice from the Designated Safeguarding Lead and refer the issue on.

12. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School, and will consider any educational benefits that they might have. The School keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

13. Sanctions

Where a pupil breaches any of the School's protocols, the Governors have authorised the Headmaster to apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include: increased

monitoring procedures, detention, withdrawal of privileges and suspension.

Expulsion is the likely consequence for any pupil found to be responsible for electronic material on his or her own or another device that would be a serious breach of School rules in any other context. Unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy.

14. Monitoring and review

All serious e-safety incidents will be logged in the E-Safety electronic log and also, if appropriate the Serious Misbehavior Register, Pastoral Register, Bullying Register.

Appendix 1 Internet protocol

1 **Introduction**

1.1 We want each pupil to enjoy using the internet, and to become proficient in drawing upon it both during your time at School, and as a foundation for your further education and career. However, there are some potential drawbacks with the internet, both for you and for the School.

1.2 The purpose of this protocol is to set out the principles which you must bear in mind at all times and also the rules which you must follow in order for all pupils to use technology safely and securely.

1.3 The rules set out below will also apply to the use of e-mail in as much as they are relevant.

2 **Use of the internet**

2.1 During School hours you must use the internet for educational purposes only to research relevant topics and obtain useful information. Access to the internet is available in the Senior School Library, Lower & Upper IT Suites as well as via a wireless network. Internet is also available in the Junior School ICT Suite.

2.2 Only at the following times may pupils access the internet at School for personal activities including communication and recreational use:

Before the start of the school day, during break times and after school subject to the other conditions within this policy.

2.3 You must not create, display, copy or otherwise distribute offensive material. Offensive material includes but is not limited to racism, sexism, pornography, bullying (including homophobic bullying), defamation, blasphemy or criminal activity including hacking. In cases of doubt, please ask any member of staff. As far as you are able, you must also make sure that you do not search for or receive such material. It is your responsibility to reject it if you come across it, and to inform a member of staff.

2.4 You must also try to protect personal and confidential information about yourself and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

2.5 You should assume that all material on the internet is protected by copyright and you must treat such material appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

2.6 Do not store executable files (.exe. files) or other copyright material such as MP3 files, wallpapers, movie clips and other formats or movie clips in your user area.

2.7 You must not bring the School into disrepute through your access to the internet. For example, you must not send or ask to receive anything which you believe the Headmaster or your parents would find inappropriate for a pupil at the School.

2.8 You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School).

2.9 Users must not attempt to reconfigure the computer, place shortcuts, aliases, software or Clip Art onto any local hard disk. Programme files must not be downloaded from the internet. Personal USB pen drives and CD-ROMs containing application software must not be brought into School.

2.10 You should treat all ICT resources responsibly, and avoid waste by not sending documents to print unless you have first previewed them, and are sure they are in final draft form. Colour printing is permitted, but pupils are expected to use this facility sparingly and not print off web pages unless absolutely necessary. All printing is monitored.

2.11 Pupils are not allowed to access interactive or networking web sites when using School computers or, if using personal laptops or other devices, on School premises.

2.12 You must not use the School's computer system to play non-educational games, or use "chat" programmes, bulletin boards, usergroups etc.

2.13 You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent inappropriate material, including personal information about someone else.

2.14 You must not load material from any disk, USB memory stick or storage device (such as an MP3 player or PSP) brought in from outside the School, unless the device has been virus checked by the School's Network Systems Manager.

Appendix 2 Email protocol

1 **Introduction**

1.1 We want each pupil to enjoy using e-mail, and to become proficient in drawing upon it both during your time at School, and as a foundation for your further education and career. However, there are some potential drawbacks with the use of e-mail, both for you and for the School.

1.2 The purpose of this protocol is to set out the principles which you must bear in mind at all times and also the rules which you must follow in order for all pupils to use technology safely and securely.

1.3 The School has systems in place that monitor and record all e-mail usage. The School reserves the right to remove the e-mail facility from any pupil who does not observe this policy.

2 **Use of email**

2.1 E-mails sent from pupils' School email accounts will be taken as representing the School and the same standards of courtesy must be applied as in the case of any other form of communication undertaken on behalf of the School. Pupils should think carefully about what is said about individuals and organisations when sending e-mails.

2.2 E-mail must be used for educational purposes only during School hours.

2.3 You must not use web based e-mail accounts such as Yahoo, Hotmail or USA.NET. This will be unnecessary as you are provided with your own personal e-mail account. You can access your School e-mail from home by going to https://mail.sionschool.org.uk then enter your username in the space provided. (the password field is your normal logon password).

2.4 You may send and receive e-mail and have access to the internet at School only during term time and only during the School day. (The School will not forward e-mails received during the School holidays.)

2.5 Appropriate authority must be obtained to send an e-mail anywhere outside of the School community.

2.6 Pupils must not read anyone else's e-mails without their consent.

2.7 Pupils must consider carefully whether to give out their external e-mail address. E-mail circulation lists operate in the same way as junk mail; continuity of service can be seriously affected by unsolicited messages, some of which may contain malicious code or virus.

2.8 Pupils should avoid sending large graphics and scanned images and must not send or receive e-mail messages, attachments or program files greater than 20 megabytes.

2.9 Pupils are responsible for their own e-mail housekeeping. Unwanted e-mails should be deleted and those to be retained should be archived regularly.

2.10 E-mailing your home e-mail address is permitted; for example to e-mail documents home to work on, then e-mailing them back to School thereafter.

3 **Misuse**

3.1 Abuse or misuse of the e-mail system will be subject to disciplinary action in accordance with Our Lady of Sion's disciplinary policy. Examples include e-mails that could be considered to be:

(a) indecent, obscene, pornographic or illegal

(b) offensive or abusive, a personal attack, rude or personally critical, discriminatory, or generally distasteful to encourage or promote activities which make unproductive use of School time

(c) involving activities outside the scope of pupils' responsibilities; for example, unauthorised selling/advertising of goods or services

(d) affecting or having the potential to affect the performance of, damage or overload the School's systems, network and/or external communications in

any way

(e) in breach of copyright or licence provision with respect to both programmes and data

(f) impersonation of another user.

3.2 You must not bring the School into disrepute through your access to the internet or e-mail. For example, you must not send or ask to receive anything which you believe the Headmaster or your parents would find inappropriate for a pupil at the School.

3.3 Any use of e-mail that is not in accordance with this policy will be dealt with as a disciplinary matter.

Appendix 3 – Mobile Devices Acceptable Use Policy

Junior School

- Pupils in the Junior School are not permitted to bring mobile devices into school. If any mobile phones are brought into school they should be handed to the office for safe keeping until the end of the school day. If a pupil is seen with a mobile phone in the Junior School, it will be confiscated and returned to the parent at the end of the school day.

Senior School

- For students in Years 7 to 11, mobile phones should be switched off and kept either in school lockers or bags during the school day. Exceptions may be permitted only in exceptional circumstances if the parent/carer specifically requests it. Such requests will be handled on a case-by-case basis and should be directed to the Headmaster. Parents/carers are requested that in cases of emergency they contact the school first so we are aware of any potential issues and may make the necessary arrangements.

- Students in Years 12 & 13 may use their phone out of sight of the main population of school. They should use phones only when absolutely necessary. Staff have the right to challenge the use.

- When express permission has been given by the teacher students may use their mobile phones in the classroom. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.

- Mobile phones should not be used to make calls, send text messages, surf the internet, take photos or use any other application during the school day unless the class teacher has given permission. This is an important aspect of ensuring our child are safeguarded during the school day.

- Using a mobile phone to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given.

- It is forbidden for students to "gang up" on another student and use their mobile phones to take videos and pictures to denigrate and humiliate that student and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student, member of staff or visitor without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

- Students should protect their phone numbers by only giving them to close friends and keeping a note of who they have given them to. This can help protect the student's number from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

- Students should mark their mobile phone clearly with their names and are advised to register their details with the network provider.

- To reduce the risk of theft during school hours, students who carry mobile phones are advised to keep them well concealed throughout the school day.

- Mobile phones that are found in the school must be handed to the school office.

- The school accepts no responsibility for replacing lost, stolen or damaged mobile phones whether in school, or while travelling to and from school.

- It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones. Students must keep their password/pin confidential. Mobile phones and/or passwords should not be shared.

- Mobile phones are banned from all examinations and controlled assessments. Students are expected to hand phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will be dealt with in line with exam board guidelines.

- Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal imagery – is also a criminal offence.

- The use of mobile phones by students on School trips is at the discretion of the trip leader.

E-Safety Policy

Chairman of Governors……..

Dated…….