ANTI - BULLLYING POLICY

What is the definition of Bullying?
An overarching definition of bullying states that it is repeated over time and intentionally hurts another pupil or group physically or emotionally and is often motivated by prejudice against particular groups, for example, on grounds of race, religion, culture, sex, gender, homophobia, special educational needs and disability, or because a child is adopted or is a carer. It may occur directly or through cyber-technology (social websites, mobile ’phones, text messages, photographs and email).

According to 'Kidscape':

- it involves aggression and unequal power relationship; and
- it results in pain and distress and is persistent.

A person is being bullied when someone else, or a group of others, sets out to make him or her miserable and unhappy. In its most serious form it can lead to psychological damage and even suicide.

Bullying, including cyber bullying, is likely to occur in all environments where a collection of people work together. Bullying may take place away from the school premises e.g. on a school bus, on the internet or a mobile phone. We have a zero tolerance policy against bullying at Doha Academy and it is our aim (pupils and staff) to eradicate bullying if it arises. To do this, we need to help the victim, the bully, the staff and parents involved.

Through PSHE your child will learn that bullying:

- Goes on for a while, or happens regularly.
- Is deliberate. The other person wants to hurt, humiliate or harm the target.
- Involves someone (or several people) who are stronger in some way than the person being bullied. The person doing the bullying has more power; they are older, stronger, there are more of them or they have some ‘hold’ over the target (e.g. they know a secret about them).

Because these three things have to happen together for something to be called ‘bullying’, they will learn that bullying is not:

- A one-off fight or argument.
- A friend occasionally being nasty.
- An argument with a friend.

Bullying is therefore:

- Deliberately hurtful
- Repeated, often over a period of time
- Difficult for victims to defend themselves against

It can take many forms but the main types are:

- Indirect – spreading nasty stories about someone exclusion from social groups, being made the subject of malicious rumours, sending malicious e-mails or text messages on mobile phones or an unpleasant comment on social network sites.
- Verbal – name calling, insulting, making offensive remarks.
- Giving looks that make the person feel uncomfortable or intimidated.
- Physical – hitting, kicking, and taking another's belongings.
- Emotional – 'being sent to Coventry' or ignored deliberately
- Deliberate/direct – cyber bullying (see policy) and the misuse of mobile phones or Internet message boards and chat rooms

Some forms of bullying are attacks not only on the individual, but also on the group to which she/he may belong. Within school we will pay particular attention to:

- Racial harassment and racist bullying.
- Bullying because of pupils' religious beliefs.
- Bullying due to gender reassignment.
- Sexual bullying of any kind.
- Bullying because of pupils' sexual orientation (Lesbian, Gay Bi-sexual Transgender (including the use of homophobic language).
- Bullying of pupils who have special educational needs or disabilities.
- Disrespect of another culture or tradition
- Cyber-bullying
- Shyness
- Lack of close friends in school

In Key Stage 1 and EYFS there can be the need to identify different strategies for dealing with bullying behaviour in younger children.

The School's Intentions

- We aim to express our belief that all pupils should be included fully in the life of the school.
- To provide a learning environment free from any threat or fear, which is conducive to the achievement of individual aspiration.
- To reduce and to eradicate wherever possible, instances in which pupils are made to feel frightened, excluded or unhappy.
- To reduce and to eradicate wherever possible, instances in which pupils are subject to any form of bullying.
- To respond effectively to all instances of bullying that are reported to us.
- To establish a means of dealing with bullying, and of providing support to pupils who have been bullied.
- To provide support for pupils who are accused of bullying, who may be experiencing problems of their own.
- To ensure that all pupils and staff are aware of the policy and that they fulfil their obligations to it.
- To ensure that all staff receive training.
- To meet any legal obligations which rest with the school.

How to recognise if someone is being bullied

A person who is being bullied is likely to be unusually withdrawn, quiet self-conscious, have a low self-esteem and appear unhappy, or the opposite may be the case. Other signs may be if a pupil:

- Becomes withdrawn and anxious
- Shows a deterioration in his or her work
- Starts to attend school erratically
- Has spurious illnesses
- Persistently arrives late at school
- Prefers to stay with adults
- Constantly seeking attention

An unusually quiet and reserved girl (or boys until 7) may try and hide the fact that she/he is being bullied by becoming more extrovert. Girls may stop eating. There may be sudden changes in her behaviour throughout the day and there may be frequent absences from school. The victim's concentration and performance in class may deteriorate. There can be psychological damage as a result of persistent bullying.

Likely behaviour of a bully

A bully can be anybody. She/he may appear aggressive, over confident, boastful and loud. However they are not always loud in their behaviour, their bullying may be quiet, very secretive and not obvious to anyone but the victim. They make you feel scared. You would find yourself trying to avoid them.

What should the victim do?
Bullies only select victims they see as weaker than themselves or as a threat to them, e.g. jealous of their popularity, appearance, talents, academic achievements or family background.

If you are being bullied:

- **REPORT IT**
- Try and stand up for yourself without being aggressive – do not be intimidated.
- Do not over-react – the bully will like to see you upset as proof of her effectiveness.

Who should you tell?
You should tell someone you feel comfortable talking to about what is happening to you, but if possible you should:

1) Tell a friend first, your Form Teacher, or another teacher. Your Form Teacher will then decide on the best thing to do to help you, which may include telling your Pastoral Manager, the Deputy Head, a member of SLT or someone older who can help you share your concern.
2) When you get home talk to a member of your family.

If you don't feel that you can do either step 1 or step 2, then:
a) Speak to our counsellor, someone who is trained to listen to your problem

Then try to practise the following strategies:
(i) ignore
(ii) stay calm and look as confident as you can.
(iii) be firm and clear and look them in the eye and tell them to stop
(iv) move away from the situation as quickly as possible
(v) remember bullying is persistent, not a one-off

N.B. Any pupil who reports a bullying incident to a member of staff will be fully supported and any subsequent intimidation by another pupil(s) will be treated equally seriously.

What should the bully be helped to do?

If you are a bully, it:

- Can become criminal behaviour. If you don't stop the police could be asked to take action. So:
- Think about the consequences to both yourself and the victim.
- Think of the hurt that you are causing; imagine how it feels to be your victim.
- Accept the help that you will be offered to face up to your problem.
- When appropriate take the opportunity to apologise for your behaviour.

What should a member of staff who sees or suspects bullying do?

Staff awareness is raised and maintained through in service training to assist them in taking action to reduce the risk of bullying at times and in places where it is most likely. There will also be reasonable consideration and appropriate adjustments made for any pupils in the School with special educational needs and disabilities, when appropriate. Teachers must be alert to the potential for bullying. If a member of staff suspects that bullying is occurring, she/he should follow the procedure below:

- Notify the Form teacher (if applicable). Please write everything down on the correct form. The Form teacher will notify the Pastoral manager and together they will deal with the situation. The Pastoral Manager will inform the Deputy Head and/or Head of Section. The Designated Safeguarding Officer keeps all records of discussion.
- The Pastoral manager will notify all relevant parties including the pupil's parents and if appropriate all staff at Staff Briefing.
- The Form teacher/Pastoral manager will investigate the situation and will talk to the victim, the bully and, where necessary, other pupils including the class of the victim and the bully.
- Be approachable for the victim/bully to talk freely. They will instigate disciplinary action where necessary and depending on the severity of the incident. This could take the form of pupil on report, regular supervision or demerits or even suspension or even permanent exclusion.
- Anonymity is important for pupils speaking to teachers but pupils must be aware that it is not always possible.
- Give the victim support and advice – offer mediation.
- Ask the child what they want you to do. How can you help them?
- Give the bully support and advice.
- Recurring bullying always involves the Head and the Designated Safeguarding Officer who will invite the parents of the bully into school for discussion.
- Proof of severe, continued bullying where sanctions are ineffective, could mean suspension or permanent removal from school. It may also necessitate the intervention of outside agencies such as the police if the behaviour continues.
- We will advise pupils responsible for bullying that we will be checking to ensure that bullying stops.
- We will keep records of incidents and record how we respond to them to enable patterns to be identified.
- A copy of the record will be kept in the files of the bullied and bully and all incidents summarised on a centrally held sheet co-ordinated by the Head of Section.

- Whistle blower harassment is treated very seriously.

What should the victim’s friends do?

- Support the victim.
- Stick up for your friend in front of the bully.
- Persuade her /him to talk to a teacher or another trusted person.
- You might feel you are able to ask the bully why she/he is behaving in this manner to your friend.
- Friends might also be intimidated by the bully, so go to a teacher/trusted person together.
- If your friend is uncertain help her to put her complaint into the concerns box or write to a member of staff they trust

What should the bully’s friends do?

- Do not join in.
- Ask her why she/he is bullying and make her think about her behaviour and the consequences.
- Offer advice on how to change this behaviour.
- Get the bully to look at the situation from the victim’s viewpoint.

What should parents do if they suspect their child is being bullied?

- Speak firstly to the Form teacher. If the Form Teacher is unable to resolve the situation, or if the seriousness of the situation requires it, he or she will then speak to the Year group leader. The Year group leader with the Head of Section or a member of SLT’s knowledge will then take the appropriate action. If unable to resolve the situation, the person responsible will speak to one of the Designated Safeguarding Officers or the Principal, as seen appropriate.
- Support your child and reassure them that the situation will be dealt with sensitively.
- Give advice but do not over react – encourage mediation where this is appropriate.

What should parents do if they think that their child is bullying?

- Ask themselves and the bully why – encourage mediation where this is appropriate.
- Contact the Form Teacher/Year group Leader/Deputy Head/Designated Safeguarding Officer/SLT/Principal.
- Decide on appropriate sanctions.
- Talk to your child about how hurtful and wrong bullying is.
- Support our anti bullying policy and procedures.
- Help them to understand that physical threats and intimidation are actually criminal offences and help them to understand how things could get out of hand.

Incident management

Doha Academy will take firm and decisive action to deal with any incident of bullying/cyber bullying which is witnessed by or reported to any member of staff by parents, pupils or staff.

Post incident responses for the victim:
When a member of staff receives information, either directly or indirectly, that a child may have been the victim of a bullying incident, this report will be taken seriously, investigated and written records kept. The incident may be investigated by the form teacher/Head of Key Stage or a senior manager.

Doha Academy will offer a proactive, sympathetic and supportive response to children who are the victims of bullying. The exact nature of the response will be determined by the particular child's individual needs and may include:

- ✓ immediate action to stop the incident and secure the child's safety
- ✓ positive reinforcement that reporting the incident was the correct thing to do
- ✓ reassurance that the victim is not responsible for the behaviour of the bully
- ✓ strategies to prevent further incidents
- ✓ sympathy and empathy
- ✓ counselling
- ✓ befriending
- ✓ assertiveness training
- ✓ extra supervision/monitoring
- ✓ creation of a support group
- ✓ peer mediation/peer mentoring
- ✓ informing/involving parents
- ✓ adult mediation between the perpetrator and the victim (provided this does not increase the victim's vulnerability)
- ✓ arrangements to review progress

Post incident responses for the bully:
Doha Academy takes bullying behaviour very seriously and will adopt a supportive, pragmatic, problem-solving approach to enable bullies to behave in a more acceptable way. Doha Academy understands that certain punishment may not be appropriate in managing this problem but the positive use of sanctions can be useful in demonstrating to bullies that their behaviour is unacceptable and encourages the promotion of positive change.

The School will respond to incidents of bullying behaviour in a proportionate way – the more serious the cause for concern the more serious the response. When sanctions are felt to be necessary they will be applied consistently and fairly. The following options will be considered:

- ➢ immediate action to stop an incident of bullying in progress
- ➢ engagement with the bully to reinforce the message that their behaviour is a breach of school rules and is unacceptable
- ➢ loss of lunch/breaktime privileges
- ➢ detention
- ➢ daily/ Head's report
- ➢ removal from class/group

- withholding participation in sports or out of school activity (if not essential part of curriculum)
- parents informed
- counselling/instruction in alternative ways of behaving
- adult mediation between the perpetrator and the victim (provided this is safe for the victim)
- fixed periods of exclusion
- permanent exclusion (in extreme cases which may involve violence)
- rewards/positive reinforcement for children in order to promote change and bring unacceptable behaviour under control.

Monitoring and Review of the Bullying policy

This policy is annually reviewed to ensure that it is working as effectively as possible. The whole school community is made aware of ways of reporting incidents of bullying. Bullying is reported to a member of school staff who will then report it to his or her line manager, and the appropriate action will be taken. A central bullying register is retained in the Head's office and is reviewed by SLT and and Head of Sections to ensure the approach by the school is effective and enables any patterns to be identified.

CONCLUSION

At Doha Academy we do not accept that bullying is an inevitable part of school life. No-one should have to suffer bullying. It is up to all of us to take action when bullying happens, to us or to others.

If the above does not solve the problem i.e. the bullying persists, suspension from school or more serious sanctions will be considered and implemented by the Head and Governors. The Designated Safeguarding Officer will be contacted in every situation.

Schedule for Development/Monitoring/Review

This E-Safety Policy was approved by the Board on:	……
The implementation of this E-Safety Policy will be monitored by the:	SLT ICT Network Manager All staff
Monitoring will take place at regular intervals:	Termly
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	June 2022
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Principal SLT DSL

The school will monitor the impact of the Policy by using:

- Logs of reported incidents
- Internal monitoring data for network activity

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school.

The internet and other digital and electronic 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 communication technologies appropriately and safely, is addressed as part of the wider duty of care to which all who work in schools are bound. DA's 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 pupil 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/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distributing 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 used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying, and Child Protection Policies).

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 and understanding to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with such risks. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

The school has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

Our E-Safety Policy has been written by the school, on government guidance. It has been agreed by the senior management and approved by Governors.

Communication with the whole school community takes place through the following:

- Staff meetings/INSET
- School Council
- Governors meetings/Sub Committee meetings
- School website/newsletters
- School assemblies

Scope of the Policy

This Policy applies to all members of the school community (including staff, students/students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspection Act 2006 empowers school leaders 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 takes place out of school.

Roles and Responsibilities

The following 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. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

A member of the Board has taken on the responsibility for E-Safety – ….

Principal and Senior Leaders

- The Principal is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Network Manager who liaises with the Senior Leadership Team on e-safety matters.
- The Principal/Senior Leaders are responsible for ensuring that the ICT Network Manager and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The ICT Network Manager reports any e-safety issues to the Senior Leadership Team.
- The Principal and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Designated Safegaurding Officer (DSL)

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT Network Manager.

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meetings of committee of Governors when required.
- Reports regularly to the Senior Leadership Team.

ICT Network Manager/Technical Staff

The ICT Network Manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the Acceptable Usage of ICT Network Policy and the E-Safety Policy.
- Users may only access the school's networks through a password procedure, in which passwords are regularly changed.
- 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.
- That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network, Virtual Learning Environment (VLE), remote access, e-mail, is regularly monitored in order that any misuse/attempted misuse can be reported to the ICT Network Manager and Principal.
- That monitoring software systems are implemented and updated regularly.

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 Use of ICT Network Policy.
- They report any suspected misuse or problem to the ICT Network Manager for investigation.
- Digital communications with students (e-mail, Portal, voice) should be on a professional level and only carried out using official school systems.
- Students understand and follow the school E-Safety and Acceptable Use Policy.

- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- 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.
- Where students are asked to research using the internet, a list of pre-checked web-sites should be given if appropriate.

Designated Safegaurding Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students

Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (N.B. in KG it would be expected that parents/carers would sign on behalf of the students).

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

- 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 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 every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

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

Policy Statements

Education – Students

The education of students in e-safety is therefore an essential part of the school's e-safety provision. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT and be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Rules for use of ICT systems/internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents/Carers

Many parents and carers have a growing understanding of e-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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- Parents' Evenings

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff is carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies.
- This E-Safety Policy and its updates are presented to and discussed by staff in staff/ team meetings/Inset days.
- The ICT Network Manager and Deputy Principal will provide advice/guidance/training as required to individuals as required.

Training – BOD

BOD should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub committees/group involved in ICT/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at local training provided by relevant bodies.
- Participation in school training/information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is a safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Use Policy and any relevant E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Network Manager and will be reviewed, at least annually.
- All users (at Primary and above) will be provided with a username and password by the ICT Network Manager, who will keep an up to date record of users and their usernames. Users will be required to change their password annually.
- The “master/administrator” passwords for the school ICT system, used by the ICT Network Manager must also be available to the Principal and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering system provided.
- The school has provided enhanced user-level filtering through the use of the Cyberoam firewall filtering programme.
- In the event of the ICT Network Manager 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 Principal.
- Any filtering issues should be reported immediately to the ICT Network Manager.

- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Network Manager and the Principal. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the SLT.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the ICT Network Manager and Senior Leadership Team.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest user type is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place (see AUP) regarding the downloading of executable files by users.
- An agreed policy is in place (see AUP) that forbids staff from installing programmes and states guidance regarding the use of removable media (e.g. memory sticks/CDs/DVDs) on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that 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.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request this by filling

in a site allowed form, available from the ICT Network Manager, who can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need, and the Principal informed.

- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

E-Safety

The growth of different electronic media in everyday life and an ever developing variety of devices including PC's, laptops, mobile phones, webcams etc place an additional risk on our children. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

Internet chat rooms, discussion forums or social networks can all be used as a means of contacting children and young people with a view to grooming them for inappropriate or abusive relationships. The anonymity of the internet allows adults, often pretending to be children, to have conversations with children and in some cases arrange to meet them.

Access to abusive images is not a 'victimless' act as it has already involved the abuse of children. The internet has become a significant tool in the distribution of indecent photographs of children and should be a concern to all those working with students at this school.

Students can engage in or be a target of bullying using a range of methods including text and instant messaging to reach their target. Mobile phones are also used to capture violent assaults of other children for circulation (happy slapping).

The best protection is to make students aware of the dangers through curriculum teaching.

Protection is Prevention

- Software is in place to minimise access and to highlight any person accessing inappropriate sites or information.
- Students will be encouraged to discuss openly their use of technology and anything which makes them feel uncomfortable. (If this results in child protection concerns the schools designated child protection person should be informed immediately)
- Students should not give out their personal details, phone numbers, schools, home address, computer passwords etc
- Students should adhere to the school policy on mobile phones.

The police will be involved if there is any criminal element to misuse of the internet, phones or any other form of electronic media.

What is CYBER-BULLYING?

- Bullying by texts or messages or calls on mobile phones
- Sexting (photographs or pictures with a sexual implication, including

  photographs of parts of a person's body in a partial or full state of undress)
- Use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, harmful, cruel or humiliating material (written or images) on web–sites or reunion sites – MySpace, MSN, PICZO, Bebo, Facebook etc or any other social networking site.
- Hi-jacking email accounts
- Making threatening, abusive, defamatory, or humiliating remarks in chat- rooms
- Hacking is a criminal act
- Harassment is completed where there is a persistent course of conduct (occurrence on at least 2 occasions) and can include the spreading of unpleasant stories about someone, exclusion from social groups or being made the subject of malicious rumours

Dealing with Cyber bullying Incidents

There is usually some visual evidence after cyber bullying has taken place. Students should be encouraged to pass this on to a member of staff or their parents. In some cases, it will be necessary to contact mobile phone companies, Internet service providers or social networking sites.

The following advice should be given to those experiencing cyber bullying:

✓ Do not retaliate or reply.

✓ Block or remove offenders from buddy lists.

✓ Review the information you are giving out.

✓ Make sure you tell an adult.

✓ Try to keep calm and do not let the bully see a reaction.

✓ Keep any evidence you have, for example text messages or print web pages.

If the person responsible for the bullying is identified, sanctions will be applied under the school's behaviour policy. In addition, the following sanctions might be implemented, depending upon the nature and severity of the bullying:

✓confiscating equipment such as mobile phones

✓withdrawing access to the Internet for a set period of time

✓limiting use of the Internet for a set period of time

✓contacting the police,

✓where the cyber bullying is sufficiently severe, informing external agencies

such as social networking or email member sites.

What should a member of staff do if they are alerted to cyber-bullying?

Notify the form teacher who with the Pastoral manager will deal with the situation and inform the the Designated safeguarding Lead and/or the Principal.

Teachers should:

1. Confiscate the mobile, **but not access its contents**;
2. Remove pupil from internet access, save material or if the event occurred at home provide evidence where possible.
3. Follow the school's E-Safety Policy
4. Be approachable for the victim /bully to speak freely. Instigate appropriate disciplinary action depending on the severity of the incident. This may be through regular supervision, banning from all use of the school internet, discussion with parent/guardian.

5. Parents/guardians will be invited into school to discuss appropriate responses.
6. Engaging in cyber-bullying could mean information being forwarded to the police and suspension or permanent removal from the school.
7. Students who use the internet in ways that cause harm to others and bring the name of the school into disrepute, may be subject to disciplinary sanctions even if the behaviour took place off school premises and even if the students are over 18.

What should the victim do?

- Tell someone as soon as possible
- Never reply to abusive messages but record/save them and report them
- Never give out personal details
- Never reply to someone you do not know
- Stay in the public areas of chat rooms
- Record/save/screen-dump any abusive or inappropriate messages.
- **REPORT IT**

What should friends of the victim do?

- Support your friend
- Go with them to tell a teacher or trusted adult and record/save any evidence.
- Do not try to sort it out yourself
- Act immediately
- **REPORT IT**

What should friends of the bully do?

❖ Do not join in

❖ Tell them to:

Respect other people’s privacy

Do not do on-line what you would not do face to face

Consider how you would feel if it happened to you

Consider how others feel

They should not cause alarm or distress deliberately or by accident

Tell them that you will inform the teacher

Don’t deal with it alone

What should parents do if their child is a victim?

If your child is a victim report it to the form teacher immediately, who will inform the Designated Safeguarding Lead and the Principal

Follow school procedure

Do not over react, but support your child and follow safe use of the internet procedure.

Use parental control software and check children use of moderated chat rooms

Screen dump or save any evidence to hand in to the school

What should the parent do if their child is the bully?

Find out why they are doing this

Explain to your child that cyber-bullying may be regarded as a criminal offence

Make sure your child understands how serious this is

Contact the form teacher/Pastoral Manager (Deans)/Deputy Principal/SLT/Principal

Remember the school operates zero–tolerance for ALL kinds of bullying

Support will be provided for the victim and the bully.

This may include meeting the bully to discuss what has happened and agree a way forward with the victim. Both will get the necessary support which is outlined in our ‘Incident Management’ section below. It is important that all children and staff recognise that when an incident of ‘cyber bullying’ takes place it is dealt with swiftly. Parents should be told, in the early stages of any bullying, what actions have been taken to remedy it and written records made.

Use of Mobile Phones in School by Children

All mobile phones should not be brought to school, if they are all mobile phones must be clearly labelled with the child's name and handed to the Operations manager immediately. It should be expressly understood and agreed that under no circumstances should the mobile phone be used during the school day, including for taking photographs. The school retains the right to confiscate mobile phones for up to 5 days if they are being used inappropriately.

Use of Mobile Phones in School by Staff and adults

Although staff and adults will bring mobile phones on to the premises, it must be understood that these should not be used for the purpose of taking photographs and they should be ***switched off*** while teaching and on silent/vibrate mode at other times.

All members of staff must be careful about giving out their mobile number and must not have pupil contact numbers in their own personal phone. Wherever possible, the school's mobile phone should be used for school trips and visits. However, there may be times when more than one phone is necessary. Where this is the case, a member of staff may use their personal phone but access to this should be restricted and agreed with the Principal or a member of SLT.

E-mailing and Instant Messaging

No member of staff may give a pupil their personal email address. Children and staff should never reply to unpleasant or unwanted emails or open files from people they don't know.

When writing emails or instant messages, think carefully about the content. When angry or distressed, you might send something likely to cause further anguish. Leave the computer and discuss the issue with someone else.

Bystanders; the issue of being a bystander or accessory is addressed with all children. Students are encouraged to respect other people on and offline and to recognise how sharing a secret and passing on numbers and passwords can cause harm and distress to others.

Being a bystander can include:

- forwarding messages
- contributing to discussions
- taking part in an online poll.

Useful advice

Useful advice can be found in the DFE statutory guidance ‘Preventing and Tackling Bullying: Advice to School Leaders, Staff and Governing Bodies.’ (July 2011). This replaced ‘Bullying – Don’t Suffer in Silence – An Anti-Bullying Pack for Schools’ and the most recent publication and resources ‘Safe to Learn: Embedding Anti-Bullying Work in Schools’. The Cyber Bullying Policy is based on the recommended guidance from the DfE ‘Safe to Learn: Embedding Anti-Bullying in Schools’ and ‘Preventing and Tackling Bullying’.

Use of digital and video games – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites and tagging them.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- ***Students' full names will not be used*** anywhere on a website or blog, particularly in association with photographs. Good practice would suggest the use of first names only.
- Written permission from parents or carers will be obtained before photographs of students/students are published on the school website. If unsure please refer to the Principal's office.
- Students' work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights

- Secure
- Only transferred to others with adequate protection

Following a number of “high profile” losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communication 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:

Cont’d over ...

	Staff and other adults				Students/Students			
Communication Technologies	Allowed	Allowed at certain	Allowed for	Not Allowed	Allowed	Allowed at certain	Allowed with staff	Not Allowed
Mobile phones may be brought to school	√							√
Use of mobile phones in lessons				√				√
Use of mobile phones after school only	√						√	
Taking photos on school camera and image capturing devices	√				√			
Use of hand held devices e.g. PDAs, PSPs	√					√		
Use of personal e-mail addresses in school, or on school network		√						√
Use of school e-mail for personal e-mails				√				√
Use of chat rooms/facilities				√				√
Use of instant messaging	√							√
Use of social networking sites				√				√
Use of blogs		√						√

When using communication technologies the school considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Staff and students/students should therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users are aware that e-mail communications may be monitored

- Users must immediately report to the ICT Network Manager; in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail

- Any digital communication between staff and students or parents/carers (e-mail, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or public chat/social networking programmes must not be used for these communications

- Students should be taught about e-mail safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate e-mails and be reminded of the need to write e-mails clearly and correctly and not include any unsuitable of abusive material

- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff

Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or disturbing 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. The school policy restricts certain internet usage as follows:

User actions		Acceptable	Acceptable at certain	Acceptable for	Unacceptable	Unacceptable/illegal
	Child sex abuse images					√

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:	Promotion or conduct of illegal acts e.g. 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				√	√
	Pornography				√	√

User Actions		Acceptable	Acceptable at certain	Acceptable for	Unacceptable	Unacceptable & Illegal
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:	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 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 (e.g. 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 under staff supervision)	√				
On-line gaming (non educational)				√	
On-line gambling				√	
On-line shopping/commerce (for educational purposes only) (staff only)			√		
File sharing (staff only)	√				
Use of social networking sites				√	
Use of video broadcasting e.g. YouTube (staff only)			√		

Acceptable Use Policy (AUP) Staff and Volunteers

Code of Conduct

Access to the School network is provided for you to carry out recognised school work and extra-curricular activities, but ONLY on the condition that you agree to follow this code of conduct.

General

- All files, including e-mail, held on the network shall be treated as school property. The ICT Network Manager and Principal can reset/update user password and examine any file or e-mail without your consent to ensure that the system is being used responsibly. You should not expect that any work or e-mail held on the school's servers will be private.
- As a network user, you are responsible for all aspects of your specific user account on the school network.
- Never reveal your password to anyone, nor let anyone use your account. If you think someone has discovered your password or is using your account, tell the ICT Network Manager or Principal immediately. Never use or attempt to use another person's account. The school keeps an audit trail of all network and internet activity and can be traced to individual user and workstation.
- You must not install, or attempt to install, any program(s) on a school computer or attempt to run any from any storage device without the express permission of the ICT Network Manager.
- You must not attempt to by-pass any network security systems, modify any profile or install registry entries.
- Always make sure that you have completely logged off from a computer before leaving it.

- Please leave your computer area and the surroundings as you would like to find them; free of any rubbish or paper.
- No computer equipment or peripherals may ever be removed from its location or tampered with. Any such interference with school property is a most serious offence.
- "Hacking" i.e. unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act, is a serious offence under Law. Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files may be considered a criminal offence under the Computer Misuse Act 1990.
- You should also be aware that the unauthorised downloading or copying of software, music etc. contrary to the provisions of the Copyright, Designs and Patents Act 1988, is not permitted.
- The installing, copying or transmitting of obscene material is forbidden and could be considered a criminal offence under the Obscene Publications Act 1959/1964.
- In addition, any material found in your user area which the school considers inappropriate or offensive will be reported immediately and sanctions applied.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

The Internet and E-mail

- Staff are, by default, given access to the Internet and e-mail. Please remember that access is a privilege, not a right, and that access requires responsibility at all times.
- The Internet is ONLY provided for you to conduct genuine research and communicate with others. All web-sites you visit, or attempt to access, can be recorded, together with the user's details, the computer that was used and the exact time and date.
- Do not use the Internet or e-mail to subscribe to "newsletter" communications using your school e-mail address, or reply to any type of "subscription form". These types of communications are forbidden and you will instantly lose your access to e-mail or to the Internet.
- Check with a member of the ICT Staff or ICT Technical Support personnel before opening **unidentified** e-mail attachments (they may contain computer viruses) or before completing any online or e-mail questionnaires.
- You must never send, display, access or try to access any obscene or offensive material.

- You must not use obscene or offensive language in e-mails. Remember that you are a representative of your school on a global public system – never swear, use vulgarities, make racial comments, or any other inappropriate language. Remember that the school has the right to read all your e-mails.
- You must never harass, insult or attack others through electronic media. Remember that any e-mail you send can be traced. Also, a recipient of an offensive e-mail from you could choose to take legal action against you.
- Never copy and make use of any material without giving credit to the author. Not only would you be infringing copyright, but you would also be guilty of theft.
- Never reveal to anyone on the Internet or by e-mail any personal information i.e. the home address or personal numbers of yourself or other students.

Sanctions

If you violate the Acceptable Use Policy, access to the Internet and e-mail will be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school ICT systems devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ____________________________________

Signed: ____

Date: ____

Please return a signed copy of this policy to the Principal.

Acceptable Use Policy (AUP) Student

The School has provided computers for use by students, offering access to a vast amount of information for use in studies, acting like an enormous extension to the School library and offering great potential to support the curriculum. Also students **with permission only** may use other devices such as laptops, tablets or other electronic devices that can connect to the internet

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources responsibly, and to help to ensure they remain available to all. Students are responsible for good behaviour with the resources and on the Internet just as they are in the classroom or a school corridor. Students should remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

Equipment

Programmes of any type must not be downloaded, installed or stored on any of the School's computers unless directed to do so by a member of staff.

Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources is not allowed and will result in computer privileges being withdrawn.

The School's computers are available to use for educational purposes only. Activities such as buying or selling goods are not allowed.

Food and drink is not allowed in the Computing rooms, the Libraries or near computing equipment.

Security and Privacy

To protect work, students must not divulge any password details or use another student's logon names/passwords.

- Student's **MUST NOT REVEAL** any personal information on the Internet (i.e. home address, telephone number, name of School or picture).
- **CYBER BULLYING IS A SERIOUS OFFENCE**. Other computer users should be respected and not be harassed, harmed, offended or insulted.
- To protect their personal security and the systems, students should respect the security on the computers and must not attempt to bypass or alter any setting.
- Computer storage areas and flash drives can be searched by staff who may review students' files and communications to ensure that the system is being used responsibly.
- The School keeps a record of all network and Internet activity which can be traced to individual users and workstations.

Internet

- Students should only access the Internet for study or authorised/supervised School activities.
- Only suitable material may be accessed. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Students should respect the work and ownership rights of people outside the School, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities, social network sites and messaging services are strictly forbidden.
- Social networking sites must not be used to display images of the School or staff or include comments that bring the staff, students or the School into disrespect or disrepute.

Laptops and iPads

Students are allowed to bring in their own devices to aid their study. These are brought into School at the owner's risk. They must be used in accordance with the Acceptable Use Policy within School and as directed by school staff. These devices can easily store images and video within the School and the owner must take responsibility for these images. It is advisable to delete all such media files when no longer needed. All videoing or taking pictures using such equipment must be authorised by a member of staff. If internet access is required on these devices permission must be gained from the member of staff teaching or supervising them.

Email

When using emails students should be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is not allowed. This applies both inside and outside School when communicating with students. The School will store and archive emails sent through the school network in order to safeguard all users within the School.

If an email containing material of a violent, dangerous, racist, or inappropriate content is received, students should **always report such messages** to a parent.

Should a pupil violate any part of the School's AUP (Acceptable Use Policy) they will be denied access to the School's Internet and be subject to disciplinary action.

Additional action may be taken by the School in line with existing policy regarding School behaviour. For serious violations, suspension or exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.

Any evidence of cyber bullying outside of school will be reported to parents and the police may be involved. Disciplinary action will be taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student Name: _____________________ Signature: ______________________

I have read and understand the above.

Parent/Guardian Name: _________________

Signature: ______________________

Date: _______________________________

Acceptable Use Policy (AUP) Year 12-13

The School has provided computers for use by students, offering access to a vast amount of information for use in studies in Grades 11 and 12.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources responsibly, and to help to ensure they remain available to all. Students are responsible for good behaviour with computing resources and on the Internet just as they are in the classroom or a school corridor. Students should remember that access is a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

In addition, Year 11 and 12 students have the privilege of bringing their own laptops, mobile phones or other computing equipment, which allows them access to computing resources and the Internet. Please note that this policy covers all these computing devices in addition to the School resources. To maintain the security of the School network, there is no direct access to the network for private devices and all Internet access via the School broadband connection is protected by filtering and firewall.

Equipment

- Programmes of any type must not be downloaded, installed or stored on any of the School's computers unless directed to do so by a member of staff.
- Damaging, disabling, or otherwise harming the operation of School computers, or intentionally wasting resources is not allowed and will result in computer privileges being withdrawn.
- The School's computing devices are available to use for educational purposes only. Activities such as buying or selling goods are not allowed.
- Food and drink is not allowed in the Computing rooms, the Libraries or near computing equipment.
- Students are responsible at all times for the use and security of any computing devices they bring into School. The School has no responsibility for these devices and students bring them in at their own risk. Students should ensure that they are suitably insured for use in School.
- The use of webcams and other digital image-capturing equipment is not allowed on School premises. Students must ensure that they disable any such capabilities before bringing computing devices into School.

Security and Privacy

- To protect work, students must not divulge any password details or use another pupil's logon names/passwords.
- Students **MUST NOT REVEAL** any personal information on the Internet (i.e. home address, telephone number, name of School, picture or any other personal information).
- **CYBER BULLYING IS A SERIOUS OFFENCE**. Other computer users should be respected and not be harassed, harmed, offended or insulted.

- To protect their personal security and the systems, students should respect the security on the computers and must not attempt to bypass or alter any setting.
- Computer storage areas, flash drives and emails can be examined by staff who may review students' files and communications to ensure that the system is being used responsibly.
- The School keeps a record of all network and Internet activity which can be traced to individual users and workstations.

Laptops and iPads

Students are allowed to bring in their own devices to aid their study. These are brought into School at the owner's risk. They must be used in accordance with the Acceptable Use Policy within School and as directed by school staff. If internet access is required on these devices permission must be gained from the member of staff teaching or supervising them.These devices can easily store images and video within the School and the owner must take responsibility for these images. It is advisable to delete all such media files when no longer needed. All videoing or taking pictures using such equipment must be authorised by a member of staff.

Internet

- Students should only access the Internet for study or authorised/supervised School activities.
- Only suitable material may be accessed. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Students should respect the work and ownership rights of people outside the School, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities, social network sites and messaging services are strictly forbidden.
- Social networking sites must not be used to display images of the School or staff or include comments that bring the staff, students or the School into disrespect or disrepute.

Email

- School email addresses may not be used for personal use.
- When using emails students should be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is not allowed. This applies both inside and outside
- If an email containing material of a violent, dangerous, racist, or inappropriate content is received, students should **always report such messages** to a parent and/or staff.
- **Should a pupil violate any part of the School's AUP (Acceptable Use Policy) they will be denied access to the School's Internet and be subject to disciplinary action.**
- Additional action may be taken by the School in line with existing policy regarding School behaviour. For serious violations, suspension or exclusion may be imposed. Where appropriate, police may be involved or other legal action taken.
- Any evidence of cyber bullying outside School will be reported to parents and the police

may be involved. Disciplinary action will be taken.

I have read and understand the above and agree to use the school ICT facilities within these guidelines.

I understand that this policy also applies to any ICT equipment I bring into school.

I have read and understand the above and agree to use the school ICT facilities within these guidelines.

I understand that this policy also applies to any ICT equipment I bring into school.

Student Name: ___________________________

Signature: ________________________

I have read and understand the above.

Parent/Guardian Name: ___________________

Signature: ________________________

Date: ___________________________________

A Guide for Staff Regarding E-safety Across the School

AIMS

This policy aims to ensure that all members of the community understand their responsibilities when using the web. It does not seek to give a comprehensive list of what is and is not acceptable. Such a list would impossible to create and maintain. In particular this policy will address expected conduct of; employees and students and parents. It will also give guidance as to the schools responsibilities for monitoring and intervening in such activities.

Employees

All employees are strongly advised to familiarize themselves fully with the privacy setting in social media, networking and blogging sites and to protect personal websites if necessary. It is particularly important to exercise good judgment when using such sites. If in doubt please seek advice from SLT.

Please note that it is never appropriate to add current students as friends, followers or similar. Previous students should only be added if they are over 18 years old **and** do not have siblings who are current students. Adding parents as friends also presents potential dangers. One should try not to do this however there may be times, for example a parent who is a long standing personal friend known separately from the professional relationship, when this is acceptable. In these cases particular care must be taken that posting do not exceed professional boundaries.

Employees, especially those in management positions, should also recognize that professional boundaries may also be strained by accepting workplace friends. Care must therefore be taken that postings respect professional boundaries. It must be remembered that school policies regarding communications between staff apply fully in the online world. All employees should remember that comments made online are likely to become known in school (**confidentiality and Facebook don’t mix well!**). Please only post information that you are comfortable for the whole community to become aware of.

In additional when publishing anything publically employees must have due regard to all school polices particularly but not exclusively those on confidentiality, harassment, discrimination, professional conduct and relationships.

The use of such personal sites is of course personal. They should not be used in school time or using school equipment. As such formal monitoring by the school of such activities would be intrusive and inappropriate. However interception and monitoring of any communications made from school or using school equipment would be considered appropriate.

Please note: That if inappropriate online behavior is brought to our attention the school has a duty to investigate fully. Where such behavior breaches current policy disciplinary measures may be taken.

Students

Students should be aware that they are expected to respect boundaries with staff and other students online as in school. In particular they should respect staff by not from making friend requests and by respecting the right of staff to a private life outside of school. We understand that social media sites and apps play an important role in the personal lives of many young people. Students should however note that inappropriate behavior or bullying within school, outside school or online will not be tolerated. The school will apply disciplinary measures when necessary in such circumstances.

Parents

Parents too are expected to respect the professional boundaries of staff and students. As with students they should avoid making online friend requests or indeed any requests that might strain these boundaries. Please note that online behavior that causes disharmony within the school environment may be investigated by the school.

All should note that it is the school's policy to involve the police if illegal activities are suspected.

General Guidance for Staff

Personal Responsibility

- DA International School employees are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time—protect your privacy.
- Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.
- Remember that information posted forms an extension of your classroom. What is inappropriate in your classroom should be deemed inappropriate online.
- The lines between public and private, personal and professional are blurred in the digital world. By virtue of identifying yourself as an DA International School employee online, you are now connected to colleagues, students, parents and the school community. You should ensure that content associated with you is consistent with your work at DA International School.
- When contributing online do not post confidential student information.
- Teachers must moderate content contributed by students.

Copyright and Fair Use

- A hyperlink to outside sources is recommended. Be sure not to plagiarize and give credit where it is due. When using a hyperlink, be sure that the content is appropriate and adheres to the DA International School policy.

- Do not use the school name or logo, nor publish photos or videos of school events without permission.

Profiles and Identity

- Remember your association and responsibility with DA International School in online social environments. If you identify yourself as a DA International School employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues, parents, and students. How you represent yourself online should be comparable to how you represent yourself in person.

- No last names, school names, addresses or phone numbers should appear on blogs or wikis.

- Be cautious how you setup your profile, bio, avatar, etc.

- When uploading digital pictures or avatars that represent yourself make sure you select a school appropriate image. Adhere to DA International School Staff Handout book guidelines as well. Also remember not to utilize protected images. Images should be available under Creative Commons or your own.

Personal Use of Social Media (Facebook, Twitter etc)

- DA Education School employees are personally responsible for all comments/information they publish online. Be mindful that what you publish will be public for a long time—protect your privacy.

- Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face, and be in accordance with the highest professional Standards.

- By ‘posting’ your comments having online conversations etc. on social media sites you are broadcasting to the world, be aware that even with the strictest privacy settings what you ‘say’ online should be within the bounds of professional discretion. Comments expressed via social networking pages under the impression of a ‘private conversation’ may still end up being shared into a more public domain, even with privacy settings on maximum.

- Comments related to the school should always meet the highest standards of professional discretion. When posting, even on the strictest settings, staff should act on the assumption that all postings are in the public domain.

- Before posting photographs and videos, permission should be sought from the subject where possible. This is especially the case where photographs of professional colleagues are concerned.

- Before posting personal photographs, thought should be given as to whether the images reflect on your professionalism.

- Photographs relating to alcohol or tobacco are deemed inappropriate. Remember, your social networking site is an extension of your personality, and by that token an extension of your professional life and your classroom. If it would seem inappropriate to put a certain photograph on the wall - is it really correct to put it online?

- Micro-blogging (Twitter etc.) Comments made using such media are not protected by privacy settings as witnessed by the high profile cases in the UK with sports stars being disciplined for tweets expressing personal views. Employees should be aware of the public and widespread nature of such media and again refrain from any comment that could be deemed unprofessional.

Social Bookmarking

- Be aware that others can view the sites that you bookmark.

- Be aware of words used to *tag* or describe the bookmark.

- Be aware of URL shortening services. Verify the landing site to which they point before submitting a link as a bookmark. It would be best to utilize the original URL if not constrained be the number of characters as in micro-blogs -- i.e. Twitter.

- Attempt to link directly to a page or resource if possible as you do not control what appears on landing pages in the future.

Instant Messaging

- DA Education School employees are not allowed to download instant messaging programs on their school computers.

- DA Education School employees must recognize this applies to instant messaging programs that are available through web interfaces with no download

- Avatar images and profile information should follow the same guidelines as the above *Profiles and Identity* section.

General Guidance for Students

The following points should be brought to the attention of students, whenever social media software is used for school activities. Teachers should ensure that points are delivered in an age appropriate manner.

1. Be aware of what you post online. Social media venues including wikis, blogs, photo and video sharing sites are very public. What you contribute leaves a digital footprint

for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.

2. Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.
3. Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.
4. Linking to other websites to support your thoughts and ideas is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.
5. Do your own work! Do not use other people's intellectual property without their permission. **It is a violation of copyright law to copy and paste other's thoughts.** When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.
6. Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or it is under “Creative Commons” attribution.
7. How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
8. Blog and wiki posts as social media projects should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.
9. If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.
10. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or access to future use of online tools.

General Guidance for Parents

Social media are powerful tools that open up communication between students, parents, and teachers. This kind of communication and collaboration can have a huge impact on learning. DA Education Schools encourages parents to view and participate by adding comments to classroom projects when appropriate.

Parents are required to adhere to the following guidelines:

1. Parents will not attempt to destroy or harm any information online.

2. Parents will not use classroom social media sites for any illegal activity, including violation of data privacy laws.

3. Parents are encouraged to read and/or participate in social media projects run by the school.

4. Parents should not distribute any information that might be deemed personal about other students participating in the social media project.

5. Parents should not upload or include any information that does not also meet the Student Guidelines as noted above

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- ***Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device***

- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Principal

- Students and staff must have permission from the Principal/Deputy Principal or Head of EYFS, Primary or Secondary before any image can be uploaded for publication

Consent of Adults Who Work at the School

- 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

Publishing Student's Images and Work

When a student enters the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site

- in the school prospectus and other printed publications that the school may produce for promotional purposes

- recorded/ transmitted on a video or webcam

- on the school's learning platform or Virtual Learning Environment

- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, ie exhibition promoting the school

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends this school unless there is a change in the student's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the ICT Manager or XXX has authority to upload to the internet following permission form the Prinaicpal or SLT has been sought.

Storage of Images

- Images/ films of students are stored on the school's network and ***(name any other media)***
- Students and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Principalteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource
- ***(name/names)*** has the responsibility of deleting the images when they are no longer required, or when the student has left the school

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are **(state who)** Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
  - Webcams can be found ***(state where).*** Notification is given in this/these area(s) filmed by webcams by signage
  - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

Video Conferencing

- Permission is sought from parents and carers if their students are involved in video conferences with end-points outside of the school
- All students are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Principal is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network

- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted

- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles

- Privately owned ICT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Data Protection Acts.

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy

- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the

ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. DA chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device

- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always ask the prior permission of the bill payer

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- *The sending of inappropriate text messages between any member of the school community is not allowed*

- *Permission must be sought before any image or sound recordings are made on the devices of any member of the school community*
- *Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used*
- *Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school*