The Yare Education Trust

IT Acceptable Use Policy

September 2016

THE
YARE EDUCATION
TRUST

IT Acceptable Use Policy

Contents

1. Preamble

The Yare Education Trust recognises that IT and the Internet are tools for learning and communication that can be used in each school to enhance the curriculum, challenge students, and support creativity and independence.

We provide students with a broad and balanced curriculum that promotes the spiritual, moral, social and cultural (SMSC) development of our students.

Students will be encouraged to regard people of all faiths, genders, races and cultures with respect and tolerance.

Our guiding principle is in the education of our community *about* ***User Responsibility*** as this enables:

- ***the educational use*** of the new e-technologies available;
- ***the respectful use*** of e-technologies with regard to the Trust's ethos and the *fundamental British values*, including *democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths; beliefs* together with gender;
- ***the safe use*** of e-technologies so that all users are kept safe from harm.

Using IT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and IT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm others. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children. Educating all members of the school community on the responsibilities and risks of online safety falls under this duty.

It is important that there is a balance between controlling access to the internet and e-technologies and allowing freedom to explore and use these tools to their full potential.

This policy aims to be an aid in regulating IT activity in school, and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online outside of school hours.

Cyber bullying by students will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in the local school Behaviour for Learning Policy and Anti-Bullying Policy, where the school has one**.**

Finally, the Computer Misuse Act 1990 identifies three specific offences:

1. Unauthorised access to computer material (that is, a program or data).

2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.

3. Unauthorised modification of computer material.

If the Computer Misuse Act 1990 is breached then a student or member of staff is likely to have the matter referred to other authorities including the police.

Online safety is a whole-school issue and responsibility. Please refer to other relevant policies, for example, policies covering Data Security etc.

2. Roles and Responsibilities

2.1 Trustees and Local Governing Bodies

The Trustees are responsible for the approval of the Acceptable Use Policy and for reviewing the effectiveness of the policy by reviewing online safety provision. The implementation of the policy is delegated to the Local Governing Bodies. Online safety falls within the remit of the Local Governor responsible for Safeguarding.

The role of the Trustees and Local Governors:

- To ensure an Acceptable Use Policy incorporating Online safety is in place, reviewed annually and is available to all stakeholders.
- The policy may be reviewed more frequently if significant changes occur with technologies in use in the schools. The online safety policy is referenced within other school policies, for example the Safeguarding and Child Protection Policy.
- To ensure that procedures for the safe use of IT and the Internet are in place and adhered to.
- To receive and challenge the annual online safety audit toward improvements, referring to the Critical Security Control checklist (NCC Online Safety Policy).
- To hold the Principal/Headteacher and staff accountable for Acceptable Use / Online safety practice.

2.2 Senior Designated IT Lead (SDITL)

The Senior Designated IT Lead will be a role delegated to a member of the Leadership Team in each school reporting to the Headteacher who has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator. In small schools the Principal/Headteacher can also be the SDITL.

Any complaint about staff misuse must be referred to the SDITL at the school or, in the case of a serious complaint, to the Principal/Headteacher.

The SDITL will:

- Ensure that there is an Online Safety Coordinator who has received appropriate CEOP training.
- Ensure access to induction and training in Online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a member of Leadership Team or equivalent.
- Ensure that student or staff personal data as recorded within the school management system sent over the Internet is secured.

- Work in partnership with the Department for Education and the Internet Service Provider and school IT Manager (or equivalent) to ensure systems to protect students are reviewed and improved.
- Ensure the school IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Ensure that the relevant Governors sub-committee will receive monitoring reports from the Online safety Co-ordinator on a termly basis.

2.3 IT Systems Manager / IT Technicians

In addition to their job description the IT Systems Manager or IT Technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body's Online Safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, the internet, the Virtual Learning Environment, remote access, and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Principal/Headteacher or Online Safety Coordinator for investigation, action, sanction or support.
- That monitoring software / systems are implemented and updated as agreed in school policies.

2.4 The IT Steering Group (Or relevant Governors Sub-committee which Considers IT and E-safety)

- This group of staff will advise, oversee and support the provision of Acceptable Use and online safety in the particular school within The Yare Education Trust.
- The school will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

2.5 Communicating School and Trust Policy

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

Rules relating to the school code of conduct when online, and online safety guidelines, are to be displayed around the school.

Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, for example during PSHEE lessons and as part of the Computing curriculum, where personal safety, responsibility, and/or development are being discussed. In the primary phases, discrete lessons are based on the materials provided by CEOP.

Staff who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues**.**

2.7 Authorising IT Access

All users must read, acknowledge and accept the '**Acceptable User Agreement' annually** before using any school IT resource. For example, through the use of a pop-up to acknowledge prior to resuming use of their IT account. This is part of the terms and conditions of working within The Yare Education Trust.

Each school will maintain a current record of all staff and students who are granted access to school IT systems.

3. Managing IT Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats.

The IT Manager or IT Technician will review the security of the school information systems and users regularly and virus protection software will be updated regularly.

Any internet resources that staff sign up to for school purposes must be done using a school email account.

Students must not be granted access to any school or online resources via personal email accounts.

Some safeguards that the school takes to secure our computer systems are:

- Working toward a system to ensure that all personal data sent over the Internet is secure, for example encrypted.
- Embedding a system so that staff are fully aware of their responsibility for ensuring that all personal data taken off site is secure.
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this.
- Files held on the school network will be regularly checked for viruses.
- The use of user logins and passwords to access the school network will be mandatory.
- Portable media containing school data or programmes will not be taken off-site unless encrypted or password protected.
- The school will support staff with choosing and using suitable passwords and help with other online safety/computer use queries.

4. Online Safety Curriculum

4.1 Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and students.

Students should be taught what internet use is acceptable and what is not and given clear objectives for Internet use as part of the curriculum. Assemblies and also class time may be used to support this.

Students should be educated in the effective use of the internet by their class teachers as appropriate and in discrete computing lessons, for example which sites to access; how to use the internet to research; not to copy and paste large chunks of the internet, how to use the CEOP Report abuse button etc.

Students will be shown how to publish and present information appropriately to a wider audience, as part of their curriculum, and as appropriate to their courses.

Online safety rules will be posted in all networked rooms including the Learning Resource Centre.

With so much information available online it is important that students learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. The students should be taught that visiting any websites and communicating online leaves a 'digital footprint'.

All users are to be aware that Internet traffic can be monitored and traced to the individual user. Discretion and appropriate conduct is essential.

Students should be taught to:

- Be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be sanctioned. If they have plagiarised in an examination or a piece of coursework, they may be prohibited from completing that examination.

- use age-appropriate tools to search for information online

- how and why to report inappropriate conduct online / unpleasant Internet content, for example using the CEOP Report Abuse icon.

Students will be informed that emails, network and Internet use will be monitored.

4.3 Managing Filtering

The school will set the guidance on the use of filtering. The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the *school Online Safety Coordinator.* Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The school will seek to ensure that the use of Internet derived materials by staff and by students complies with copyright law.

The school will work in partnership with Norfolk Children's Services to ensure systems to protect students are reviewed and improved.

For more information on data protection in school and across the Trust, please refer to our Data Protection Policy.

More information on protecting personal data can be found in Section 9. of this policy.

4.4 Parental Support

Parents' and carers' attention will be drawn to the Online Safety Policy on enrolment of their child, in newsletters, and on the school website.

Parents and carers will from time to time be provided with additional information about online E-safety.

Acceptance of a place at a school within the Trust and subsequent enrolment confirms the agreement of parents and students to support and abide by all school policies and procedures in place and as varied from time to time.

4.5 Handling Online Safety Complaints

Any complaint about staff misuse must be referred to the SDITL at the school or, in the case of a serious complaint, to the Principal/Headteacher. If the complaint is about misuse by the Principal/Headteacher, it must be referred to the Chair of Governors.

Complaints of Internet misuse by students will be dealt with:

- at primary phase – by the appointed member of the school Leadership Team
- at secondary phase – by the pastoral leader for that student, for example, a Head of House or Class Teacher in conjunction with other staff as appropriate.

Concerns of a safeguarding nature must be referred to the Designated Safeguarding Lead and their team and dealt with in accordance with school procedures.

5. Cyber Bullying

The school, as with any other form of bullying, takes Cyber bullying seriously. Information about specific strategies to prevent and tackle bullying is set out in the **Behaviour for Learning Policy** and the **Anti-Bullying Policy.**

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

If an allegation of bullying involving the use of IT or any emerging technology does take place, the school will:

- Follow the policy and procedures for dealing with bullying
- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the person causing concern
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the person causing concern that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the person causing concern will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

6. Use of Email

It is important that users of our email systems should be confident about the following:

- The identity of the user of the email account with whom they are communicating
- The security of the communications and any data sent
- That the school has access to an audit trail of the conversation in the event of any issues arising.

6.1 Staff Use of Email

Staff school email accounts should be used for any and all school business and most especially when communicating with students, parents and external organisations and individuals on school business.

Be aware that emails have legal force, for example what you say in an email has as much legal standing as something you write on paper.

Personal email accounts should not be used in a professional capacity. Equally, school email accounts must not be used for any personal matters or use, which includes signing up to subscriptions services.

Incoming email should be treated as suspicious and attachments not opened unless the author is known.

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

The forwarding of chain messages is not permitted in school.

6.2 Email Communication with Students

Staff must only have email contact with students using their school accounts.

Students must use only their school email accounts to contact staff.

If a student emails from a personal email address staff may reply but only to ask them to use their school email address for communication.

People not employed by the school but communicating with students for school purposes must use a verifiable business email account not a personal email account. If they do not have one then the school will provide one.

6.3 Student Email

Students may only use approved email accounts on the school system.

Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone unknown.

Students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Incoming email should be treated as suspicious and attachments not opened unless the author is known.

The school will monitor how email from students to external bodies is presented and controlled:

- primary phase – all emails going to an outside agency or person, must be checked by a teacher first
- secondary phase - students should copy in the supervising teacher.

Students will be educated through the IT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

6.4 Email Communication with Parents

Email communication with parents should occur only to the email address registered to them in the school MIS.

Reference should be made to the Data Protection Policy to ensure compliance.

Confidential information must ***not*** be sent by email to parents as our emails are not encrypted.

6.5 Internet Resources

Internet resources that users sign up for school purposes must be done using a school email account and logged centrally.

Students must not be granted access to any resources using any form of personal email accounts.

7. The School Website

The contact details on the website should be the school address, email and telephone number.

Staff or students' personal information will not be published.

7.1 Published Content

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school and personal achievements, and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published.

8. Social Networking

The school will control access to social networking sites, and will educate students in their safe use, for example use of passwords and security/privacy settings.

All students will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

Students must not place personal photos on any social network space provided in the school IT resources without permission.

Students, parents and staff will be advised on the safe use of social network spaces.

Students will be advised to use nicknames and avatars when using social networking sites.

8.1 Social Media, Social Networking and Personal Publishing on School IT Resources

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. *There are various restrictions on the use of these sites in school that apply to both students and staff.*

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

- Students are educated on the dangers of social networking sites (including gaming sites) and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of IT and technologies and behaviour online.

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

- Official school blogs created by staff / students for the school IT resources are not to be publicly visible unless approved by the Principal/Headteacher or relevant Governors' sub-committee. They will be moderated by a designated member of staff.

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

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

9. Data

9.1 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

The school will follow these principles of good practice when processing data:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities and companies associated with a service provided to the school; for example, our local authority, Ofsted, or the Department of Health. The school will ensure that these authorities/companies are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the Trust and school’s safeguards relating to data protection please refer to the Data Protection Policy.

9.1 File Sharing Services

With any service that shares files, for example Google, do not "share" any files unless you are confident about how the system works, and who will be able to access the data. Any files containing personal data of staff or students should be uploaded onto the file sharing network.

Key Example

All school-related Google material must at every stage be created and worked on via the school Google account (not a private account). This is partly because shared files originating "at home" will carry the home account email on them, even after "sending" them to school. This is different to more unified systems such as Microsoft.

9.2 Images

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

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

It is important that published images do not identify students or put them at risk of being identified.

Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

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

Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a home school agreement including photography consent. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect the use to which you are consenting.

Photographs that include students will be selected carefully and the school will look to seek to use group photographs rather than full-face photos of individual children.

Students' full names will be avoided on publicly accessible school IT resources as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Staff and external parties will be made aware of the restrictions on photographing certain students through the website and relevant policies.

9.3 Complaints of Misuse of Photographs or Video

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

9.4 Use of Photography and Filming at School Events

All schools in the Trust will follow the NCC guidance for schools – 'Guidance for schools: Parents and Carers use of photography and filming at school events.

10. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are they:

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

The school takes certain measures to ensure that mobile phones are used responsibly in school.

At primary phase:

- Parents must write to the school, explaining why the child needs their mobile phone in school and the school will store the phones during the school day. Children must hand these in at the start of every school day and they can then be collected at the end of the school day through the individual school's system. Should a child knowingly not hand their phone in at the start of the school day, this issue will be managed through the school's Behaviour Management Policy.

At secondary phase:

- Mobile phones and associated cameras will not be used during lessons except as part of an educational activity at the discretion of the teacher.
- The school will not tolerate cyber bullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **School Behaviour Policy.**
- Images or files should not be sent between mobile phones in school.
- A member of staff can confiscate mobile phones if used inappropriately.
- A member of the Leadership Team can search the device if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Any student who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- If staff wish to use these devices in class as part of a learning project, they must follow the above guidance.

Staff should not share personal telephone numbers with students and parents. A school telephone will be provided for staff where contact with students is required.

Staff MUST NOT use personal devices such as tablets, mobiles and personal laptops to access school systems, without explicit permission from the Principal/Headteacher.

Students

- Students who breach school policy relating to the use of personal devices will be sanctioned in line with the school's Behaviour Policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that examination.

Staff

- In nurseries, staff are not permitted to bring their mobile phones into areas used by children. Personal belongings, including mobile phones, should always be stored in the nursery office.
- Staff should not use their personal mobile phones to contact students or parents either in or out of school time for any school-related purpose. The only exception would be in an emergency and it would need to be logged with the Office.
- Staff are not permitted to take photos or videos of students on their personal phones. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment should be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

11. Managing Emerging Technologies

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

Appendix 1 - The Acceptable Use Agreement - Staff and Governors

To ensure that members of staff are fully aware of their professional responsibilities when using information and communication systems equipment, staff are asked to sign this code of conduct. Members of staff must read and understand the school's e-safety policy prior to signing.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.

I understand that it is a disciplinary offence to use any school ICT system or equipment for a purpose not permitted by its owner.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email and social networking. ICT use may also include personal ICT devices with the permission of the Principal if used for school business.

I understand that school information systems and equipment may not be used for private purposes.

I understand that my use of school information systems, internet and email is monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose or share any password or security information to anyone. I understand that I will be deemed responsible for any activity undertaken through my user account.

I will not install any software or hardware without consulting the System Manager first.

I will ensure that personal data is stored securely and is appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding the inappropriate use of ICT systems or equipment to the ICT Co-ordinator, E-safety co-ordinator, the designated Child Protection Officer or the Principal.

I will ensure that all electronic communications I make are compatible with my professional role.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed……Name……Date……

Accepted for School:……Name……

Please ensure you have read sections 12, 14, 27 and 28 of the "Guidance for Safer Working Practice for Adults Who Work with Children and Young People" document.

Appendix 2 - The Acceptable Use Agreement - Students

The school computer network is provided to enhance learning and to aid teaching whilst making it more enjoyable.
It is important that the equipment is used safely and appropriately.
The following are breaches of Network and Internet rules with consequences (**in bold**).
At any time, a student could be excluded through their misuse of the system or have their Internet access denied.

I understand that I must not:-

1. Allow anyone to know my password for any reason.
2. Allow anyone to access the network and/or the Internet as a user other than themselves, whether they are banned or not, under my user name and password.
3. Attempt to access files or folders outside of my personal folder, public area or clipart.
4. Tamper with or damage computer equipment in any way.
5. Install or attempt to install, programs of any type on a machine or storing programs on the computers without permission.

If I break these rules, the class teacher will record the incident and the teacher or the Curriculum Leader will punish me.

I understand that I must not:-

Use chat, network chat or messenger services on the Network or the Internet.
Use the Network/Internet for commercial purposes e.g. buying and selling of goods.
Access non-work related material other than correspondence sites such as web-mail.

If I break these rules, the class teacher will record the incident and I will be given a detention.
My parents will be informed through a letter stating why I have a detention.

I understand that I must not:-

8. Bypass or attempt to bypass the Internet security in place.
9. Type an unsuitable word into a search engine and/or type an unsuitable URL (website address) into the address bar. ("Unsuitable" is defined as words/statements relating to computer based games (including consoles), material of a sexual nature, obscene/swear words, items relating to non-conformist groups or groups of questionable origin/ beliefs/political views, words that can be construed as racist or bullying.)
10. Have, place or attempt to place unsuitable material:
    - On a CD/USB device or any other storage medium in school.
    - In my user folder on the network.
    - In a shared network area such as 'Students'.
    - On a laptop/palmtop or other electronic device in school.
11. Pursue or attempt to pursue unsuitable results from a search of the above type. View or attempt to view or download any unsuitable results.
12. Enter or attempt to enter a suspect site.
13. Download or attempt to download any unsuitable material in any electronic format.
14. Send or attempt to send any unsuitable material using any type of e-mail.

If I break these rules, the class teacher will report the incident and my parents will be contacted and asked to come in for a meeting with either my Head of House or the Vice Principal.
An ICT Community Service Detention will be set.

I also understand that if I hack into or use the school system inappropriately, my parents will be informed and asked to attend a meeting with the Vice Principal and School Network Manager.
At that meeting, appropriate action will be decided.

Finally, I understand that I must report any serious misuse of the computers/systems to my class teacher or form teacher as soon as possible.

PARENT/GUARDIAN: I have read and understood the AUP. I accept that the responsibility to adhere to the policy is that of my son/daughter and a breach of any of the conditions above will lead to the indicated actions being taken.
I hereby give my permission to use the school computer network facilities, including the Internet.

Parent/guardian signature……Print name……

STUDENT: I have read and understood the AUP. It is my responsibility to exercise common sense and caution when using the computers in school. It is my responsibility to abide by the AUP above and I understand that if I do break the rules I will be subject to sanctions. I understand that I may only use the school computers for schoolwork.

Student signature……Print name……..

Appendix 3 - The IT Services Code of Conduct

Preamble

The school employ specific staff to administer, develop and run the school IT systems. Of necessity these staff have sweeping powers and access rights across the systems which are needed for effective day to day running of the network. This document lays out a code of conduct for those staff. This document is in addition to the standard Code of Conduct.

Scope

This Code of Conduct applies both to the staff that specifically support the wider school IT network and resources and also to those who have authority over specifics applications, systems or web resources with regard to those specific resources.

Authority

The Principal/Headteacher and the Local Governing Body delegate full authority for accessing, managing and running the school IT network and associated system to the IT Services Manager / IT Technician. He in turn delegates that authority to members of the IT team as needed to perform their duties. This authority will not be delegated outside the IT team without the Principal's/Headteacher's permission.

Confidentiality

During the course of their work, administrators are likely to become aware of information which is or may be regarded as confidential. Unless it raises a safeguarding concern, any such information must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation or legitimate authorised request. Administrators may not browse areas of the network or school resources for any purpose than fulfilling their job.

Assumed Authority

If a user requests assistance from the IT team, the user's authorisation to access those areas covered by the issue being investigated will be assumed. This authority will extend no further than that required to deal with the specific issue.

Access to Personal Areas

In exceptional circumstances a member of staff's line manager or the Principal/Headteacher may request temporary access to areas normally accessible only to that user (for example, email or home folders). All such requests must be logged so they can be reported on at a later date if required.

System Logins

System logins will only be created for staff and students who have passed through the approved admission and authorisation channels. In practice this means they will need to have an entry on the school MIS system. Guest users may be granted temporary access for limited, defined periods of time with no access allowed to staff resources. Other access arrangements must be approved on a case by case basis by the Principal/Headteacher and recorded.

Access to School IT Resources and Files

Authority for access to files and resources that the school owns is delegated to the managers of the respective departments or persons who are otherwise responsible for those resources. Permission must be sought and obtained from them or the Principal/Headteacher before access is granted.

Exceptional Circumstances

In exceptional circumstances where immediate action is required to protect the network, data or any person or if no one is available to give authorisation (for example, during school holidays), the IT team may act without such authority. All such instances of such action must be reported to the Headteacher at the earliest opportunity.

Appendix 4 - Network Etiquette and Privacy – A Guide

All members of our school communities are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

BE POLITE. Never send or encourage others to send abusive messages.

USE APPROPRIATE LANGUAGE. Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

PRIVACY. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.

PASSWORD. Do not reveal your password to anyone. If you think someone has obtained your password, change it, and contact a member of the IT Team or your teacher.

ELECTRONIC MAIL. Electronic mail (email) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.

DISRUPTIONS. Do not use the network in any way that would disrupt use of the services by others.

OTHER CONSIDERATIONS:

- Be brief. Few people will bother to read a long message. Proof read your message to ensure that it is error free and easy to understand.
- Remember that humour and satire are very often misinterpreted.
- Cite references for any facts that you present. Do not copy work and imply that it is your own. If you do so you are almost certainly guilty of plagiarism. Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.
- Respect the rights and beliefs of others.

Appendix 5 - Model Union Guidance

ONLINE SAFETY: PROTECTING SCHOOL STAFF

This document provides a brief guide on how to stay 'Cybersafe'.

Online safety is a key issue for all schools as it can pervade all aspects of school life. Staff in schools, as well as students, may become targets of 'cyberbullying'. Cyberbullying is a whole school community issue. It takes place when an individual or group of people use technology such as the internet, mobile phones, email, chat rooms, or social networking sites to bully, threaten or embarrass their victim. It is important that schools make it clear that bullying including cyberbullying of staff is unacceptable.

The following information provides the 'do's and don'ts' on how to stay 'Cybersafe', taking into account the unique position that a teacher or associate staff member has in the school and wider community:

Teachers / Associate Staff should:

- not post information and photos about yourself, or school-related matters, publicly that you would not want employers, colleagues, students or parents to see;
- not leave a computer logged in when you are away from your desk and keep passwords secret and protect access to accounts;
- not befriend students or ex-students of school / college age on social networking sites. (You should also consider carefully the potentially adverse implications of befriending parents or adult ex-students – indeed Department for Education advice is to not befriend ex-students at all. There are clear reputational and other risks associated with linking with parents and / or adult ex-students on social networking sites and the member of staff is advised to make themselves as fully informed as possible of those risks, for example by speaking with the Principal/Headteacher.)
- keep personal phone numbers private and not use your own mobile phones to contact students or parents;
- use a school mobile phone when on a school trip;
- keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school premises and report thefts to the police and mobile operator as soon as possible;
- ensure that school rules regarding the use of technologies are consistently enforced;
- not personally retaliate to any incident;
- report any incident to the appropriate member of staff in a timely manner (usually a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of cyberbullying incidents);
- keep any evidence of an incident, for example by not deleting text messages or e-mails and by taking a screen capture of material, including the URL or web address;

- use school e-mail address only for work purposes;

- be aware that if you access any personal web-based e-mail accounts via your school network, that these may be subject to the school's internet protocol which could include monitoring and surveillance;

Teachers / Associate staff should recognise that laptops provided by the employer are for employer's business only, and are not the personal property of staff and therefore should not also be used by family members or for personal activities. Schools should make reasonable attempts to ensure that staff know the risks and dangers of inappropriate internet use

Useful Resources

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material the staff member should use the tools on the social networking site directly to make a report. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is, for example by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected to be illegal you should contact the police directly.

Contact details for social networking sites:

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools. Advice can be found here http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers/safety-tools-on-online-services

Facebook Read Facebook's Rules Report to Facebook Facebook Safety Centre	**YouTube** Read YouTube's Rules Report to YouTube YouTube Safety Centre
Instagram Read Instagram's Rules Report to Instagram Instagram Safety Centre	**Twitter** Read Twitter's Rules Reporting to Twitter
Vine Read Vine's Rules Contacting Vine and Reporting	**Kik Messenger** Read Kik's Rules Reporting to Kik Kik Help Centre
Ask.fm Read Ask.fm's 'Terms of Service' Read Ask.fm's Safety Tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.	**Tumblr** Read Tumblr's Rules Report to Tumblr by Email If you email Tumblr take a screen shot as evidence and attach it to your email.

Mobile Phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. They can help you to change the number of the person being bullied if necessary. It is not always possible for operators to block particular numbers from contacting the person being bullied, but many phones, such as IPhones allow users to block phone numbers.

If you want to prosecute the individual contact the police. If a bully is making direct threats which you feel constitute a real danger, phone 999. If there is not an immediate danger, then contact the non-emergency number 101. The mobile provider can work closely with the police and can usually trace malicious calls for them.

Contact Details for Service Providers:

Service Provider	From Your Mobile	Pay as You Go	Pay Monthly Contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751