E-SAFETY POLICY

This policy is regularly reviewed following recommended guidelines.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and governors
- Ensure that parents/carers are actively involved in the school's approach to online safety
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The Governing Body will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understood this policy
- Ensure that the school follows all current e-safety advice to keep children and staff safe
- Support the school in encouraging parents/carers and the wider community to become engaged in e-safety activities

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school in conjunction with the E-safety Coordinator, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS
- Ensuring that any incidents of cyber-bullying are logged through SIMS and dealt with appropriately in line with the school's behaviour policy
- Updating and delivering staff training on online safety, ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher/Senior Leaders and/or Governing Body
- Keeping up to date on e-safety legislation, and be aware of the potential for serious child protection issues to arise from; sharing personal data, access to illegal/inappropriate material, inappropriate online contact with adults/behaviours, potential or actual incidents of grooming, cyber-bullying and use of social media

This list is not intended to be exhaustive.

The aims of safeguarding within this policy run parallel with those in the Child Protection and Safeguarding Policy. The protocol on incidents of Safeguarding are available in the Staff Handbook.

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and are communicated directly with the Designated Safeguarding Lead
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Report any e-safety related issues that arise, to the E-Safety Coordinator to ensure that users may only access the School's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- Ensuring that access controls and encryption exist to protect personal and sensitive information held on school-owned devices
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and are tested at regular intervals to demonstrate their effectiveness
- Keeping up-to-date documentation of the School's e-security and technical procedures
- Providing guidance to teachers and learners on their use of the Internet and e-mail
- Ensuring all Learners agree to the iPad AUP Prior to accessing the school iPad

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Procedures that need to be followed in the event of an e-safety incident
- Adhering to this policy, and ensuring that learners follow the school's terms on iPad acceptable use (Appendix 3)
- Working with the DSL to ensure that any online safety incidents are logged via the online E-Safety Incident Form (Appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Reporting any suspected misuse or problem to the Headteacher/Line Manager/ Designated Safeguarding Lead/Cohort Leader/Network Manager for investigation/ action/consequence
- Ensuring all digital communications with learners, parents/carers should be on a professional level *and only carried out using official school systems*
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

In addition, teaching staff are expected to:

- Embed e-safety issues in all aspects of the curriculum and other school activities
- Supervise and guide learners carefully when engaging in learning activities involving online technology (including extra-curricular and out of school activities if relevant)
- Ensure that learners are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- In learning sessions where internet use is pre-planned, learners 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

This list is not intended to be exhaustive.

3.6 Learners

Learner responsibilities and expectations:

- To read, understand, sign and adhere to the iPad Acceptable Use Policy (Appendix 3)
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To know and understand school policy on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policy on the taking / use of images and on cyber-bullying
- To 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
- To keep all personal details secret – this includes passwords. Learners are responsible for any misuse of their password. Learners are encouraged to regularly change their passwords to protect privacy
- To access the internet and emails appropriately during learning sessions for educational purposes only
- School staff may access any file held on any computer storage system or media that is part of or connected to the school network. The school reserves the right to access any portable electronic storage device or other media brought into school and to monitor all communications. Learners should thus be aware that their files will not always be private
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home

3.7 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on the iPad Acceptable Use Policy, (Appendix 3) guidelines for Learners' Internet Access document (Appendix 4) and the Internet Policy (Appendix 5)
- Communicate with the school if they have any concerns about their child in relation to any aspects of e-safety
- Be responsible for the security/filtering controls at home (if support is needed with this, contact the Network Manager)

Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Learners and parents/carers are provided with documents as part of the school's admission process, these documents include; Internet Permission (Appendix 2) iPad Acceptable Use Policy (Appendix 3) Guidelines for Learner's Internet Access (Appendix 4) and Internet Policy (Appendix 5).

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating learners about online safety

Learners will be taught about online safety as part of the curriculum. Specific sessions are dedicated in year 7 as part of the IDEA design for learning and aspects of this are covered in learning session 5 as part of the PSHE curriculum as well as within the GCSE course for Computer Science.

Learners will be taught:

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

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The main areas of risk can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

The safe use of social media and the internet will also be covered in other subjects where relevant. There is also a comprehensive programme which is taught through Learning Session 5. Further details can be found in the RSE and PSHE policies.

The school may use assemblies to raise learners' awareness of the dangers that can be encountered online and may also invite speakers to talk to learners about this.

5. Educating parents/carers about online safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, such as headlines and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during the Cohort 7 meet the Learning Group Leader in the Autumn term.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Cohort Leader/DSL and/or the Headteacher or member of the Senior Leadership team.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See the school's Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Learning Group Leaders will discuss cyber-bullying with their Learning Group as part of the RSE/PSHE curriculum, and the issue will be addressed in assemblies when necessary.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal, Social, Health and Economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The school also shares information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on learners' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and in line with school's behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the school complaints procedure.

7. Learners using mobile devices in school

Learners may bring mobile devices into school, but are not permitted to use or access their mobile phones during the entire school day, including break and lunch times. Once learners enter the school site phones and other electronic devices must be away (until phones are handed in during AM registration). The same rules and expectations apply for learners that attend before/after school revision clubs/interventions and Independent Study club. Any breaches in the use of mobile phones is responded to in line with the school behaviour policy.

Learners are provided with an iPad and are subject to the terms and conditions as set out in the iPad Acceptable Use Policy (Appendix 2) Any breach of the acceptable use agreement by a learner may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device or other restrictions placed on it.

8. Staff using work devices outside school

Staff members are permitted to use personal or work devices inside and outside of the school.

Staff must ensure that their personal/work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any external portable storage devices such as memory sticks or hard drives need to be submitted to the Network Manager prior to use so that they can be encrypted. Technical restrictions will be put in place so that it is not possible to "WRITE/SAVE" new data to an unencrypted memory stick but it will be possible to "READ/OPEN" from them.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would damage it. Access to the Internet from an employee's home using a school owned device or through school owned connections must adhere to all the policies that apply to their use. Family members or other non-employees must not be allowed to access the school's computer system or use the school's computer facilities, without the formal agreement of their Line Manager.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

9. How the school will respond to issues of misuse

Where a learner misuses the school's iPads, ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Staff will log the incident on SIMs (the school's data system) and log on CPOMS if the incident is related to safeguarding and inform the Designated Safeguarding Lead/Network Manager/Cohort Leader/Senior Leader.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Use of IT systems/equipment, E-mail and the Internet

All learners, parents/carers, staff, volunteers and governors using the school's electronic mail services including Google suite platforms and/or the Internet are expected to do so responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

Computers, laptops and tablets loaned to employees by the school are provided to support their professional responsibilities. Employees must not use school equipment or property for personal gain or fraudulent, malicious, illegal, libellous, immoral, dangerous, offensive purposes. Employees should not undertake IT related activities that are contrary to the school's policies or business interests including accessing, downloading, storing, creating, copying or distributing offensive material (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

All forms of chain mail are unacceptable and the transmission of user names, passwords or other information related to the security of the school's computers is not permitted.

10.1 Personal use (All staff and volunteers)

The school's e-mail and Internet service may be used for incidental personal purposes, with the approval of the Line Manager, if it does not:

- Interfere with the school's operation of computing facilities or e-mail services
- Interfere with the user's employment or other obligations to the school
- Interfere with the performance of professional duties
- Is of a reasonable duration and frequency
- Does not overburden the system or create any additional expense to the school
- Does not bring the school and its employees into disrepute

Such use must not be for:

- Unlawful activities;
- Commercial purposes not under the auspices of the school
- Personal financial gain
- Personal use that is inconsistent with other school policies or guidelines

If an employee fails to meet these conditions for personal use, their rights to use equipment may be withdrawn. If an employee fails to follow this policy and other supporting procedures, this could result in disciplinary action.

10.2 Privacy

The school respects users' privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by law.
- If there is a substantiated reason to believe that a breach of the law or school's policy has taken place.
- When there are emergency or compelling circumstances.

The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies. Monitoring will be reasonable and in accordance with Data Protection and Human Rights obligations.

Employees should not have any expectation of privacy to their internet usage. The school reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

Use of the employee's designated personal file area on the network server provides some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to policies and to the law. The employee's personal file area is disk space on the central computer allocated to that particular employee. Because it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available to the whole staff or wider school community.

Managers will not routinely have access to an employee's personal file area. However, management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

10.3 Email/IT Protocols

A good practice guide for employees is available on the use of Emails (Appendix 6).

Users must:

- Respond to Emails in a timely and appropriate fashion. The system is designed for speedy communication. If urgent, the e-mail requires a prompt response, otherwise a response should be sent within a reasonable timeframe according to the nature of the enquiry
- Create group emails for sending information to learning groups, classes etc

- Use the appropriate email codes to enable learners to filter their emails, which have been made available to staff through the Staff Bulletin
- Not use anonymous mailing services to conceal identity when mailing through the Internet, falsify Emails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details
- Not abuse others (known as 'flaming'), even in response to abuse directed at themselves
- Not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system
- Not use, transfer and tampering with other people's accounts and files
- Use their own devices and equipment to connect to the school/school's network, but should liaise with the IT team to ensure the equipment meets appropriate security and other standards. Under no circumstances is personal equipment containing inappropriate images or links to them, to be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children
- Ensure that learners are not exposed to any inappropriate images or web links. School/Service and adults need to ensure that Internet equipment used by children have the appropriate controls with regards to access, e.g. personal passwords should be kept confidential. Staff should under no circumstances allow learners to access systems via their accounts
- Not store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices
- Respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner
- Not use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations

If a user finds they are connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate Internet sites must be reported immediately to their Line Manager. Any failure to report such access may result in disciplinary action.

Except in cases in which explicit authorisation has been granted by the Headteacher, employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties
- Hacking or obtaining access to systems or accounts they are not authorised to use
- Using other people's log-ins or passwords
- Breaching, testing, or monitoring computer or network security measures
- Interfering with other people's work or computing facilities

10.4 Security

The school follows sound professional practices to secure email records, data and system programmes under its control. As with standard paper-based mail systems, confidentiality of email cannot be 100% assured. Consequently, users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered that emails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

In order to effectively manage the e-mail system, the following should be adhered to:

- Open mailboxes must not be left unattended
- Care should be taken about the content of an email as it has the same standing as a memo or letter. Both the individual who sent the message and/or the school can be sued for libel
- Report immediately to IT units when a virus/malware/phishing is suspected in an email

10.5 Social Networking

The purpose of this part of the policy is to ensure that:

- The school is not exposed to legal and governance risks
- The reputation of the school is not adversely affected
- Our users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of the school
- Protocols to be applied where employees are contributing in an official capacity to social networking applications provided by external organisations

Social networking applications include but are not limited to:

- Blogs i.e. blogger
- Online discussion forums, for example Facebook, Instagram
- Media sharing services for example YouTube
- 'Micro-blogging' application for example Twitter

10.6 School/Academies Managing Social Networking Sites

This may include internal forums for staff and outward facing forums for school activities/clubs etc.

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official school purposes. To assist with this, all employees must adhere to the following requirements:

- Only use an official (i.e. not personal) e-mail addresses for user accounts which will be used for official purposes
- Appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users
- The school's logo and other branding elements should be used where appropriate to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position
- Employees should identify themselves as their official position held within the school on social networking applications. e.g. through providing additional information on user profiles
- Employees should ensure that any contributions on any social networking application they make are professional and uphold the reputation of the school – the general rules of internet/email apply
- Staff should not spend an unreasonable or disproportionate amount of time during the working day developing, maintaining or using sites;
- Employees must not promote or comment on personal, political, religious or other matters
- Employees should be aware that sites will be monitored.

10.7 Personal Social Networking Sites

All employees of the school should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation and the Safeguarding Vulnerable Groups Act 2006. Employees must also operate in line with the school's Equality policy.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the school community. Employees hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the school, any of its employees or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.

Employees should not use personal sites for any professional activity. The school reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the school or put it at risk of legal action.

Anyone who becomes aware of inappropriate postings on social networking sites, must report it to their Line Manager as soon as possible. The Line Manager will then follow the disciplinary procedure. If an employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this policy, then that employee may be subject to the disciplinary procedure.

10.8 Posting Inappropriate Images, video or comments

Indecent images of any employee that can be accessed by learners, parents/carers or members of the public are totally unacceptable and can lead to child protection issues as well as bringing the school into disrepute.

It is totally unacceptable for any employee to discuss learners, parents, work colleagues or any other member of the school community on any type of social networking site.
Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

10.9 Social Interaction with Learners (Past and Present)

Employees should never communicate with any current learner using a social networking site (only use school email address).

Any communication with a former learner should be via a school email account. If staff do use private communication tools to communicate with former learners, this must only be once that learner has reached their nineteenth birthday, or, in the case of a learner they have taught at sixth form once that learner has left the sixth form and ceased to be taught by them for at least two years.

Employees are liable for all communication which could affect their work and the school and accept, therefore, that disciplinary measures could be taken against them where their use of any social networking site, or any other electronic communication, negatively affects the school, its learners or other employees.

Adults should ensure that personal social networking sites are set private and that current learners are never listed as approved contacts and only former learners following the guidelines above.

Adults should not use or access social networking sites of learners. However, it may be required for members of the IT Team to do this under direction of the Headteacher if it is required for safeguarding purposes.

Should an employee become aware of an underage person using social networking sites, (Facebook has set it at 13 years and Myspace has set it at 14 years), then they should report this to the Cohort Leader and their Line Manager who will contact parents to discuss.

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. Again, this may leave employees vulnerable to allegations being made.

10.10 General Terms of Use

All employees must adhere to the following terms of use of social networking applications. This includes, but is not limited to public facing applications such as open discussion forums and internally-facing applications, regardless of whether they are hosted on organisational networks or not. The school expects that users of social networking applications will always exercise due consideration for the rights of others and strictly in accordance with the following terms of use. Social networking applications must not be:

- Used to publish any content which may result in actions for breach of contract, defamation, discrimination, breaches of copyright, data protection, breach of confidentiality, intellectual property rights or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school or the Trust into disrepute.
- Used for the promotion of personal financial interests, commercial ventures or personal campaigns unless approved by the Headteacher;
- Used in an abusive or hateful manner;
- Used for actions that would put other employees in breach of the Code of Conduct Policy;
- In breach of the school's Staff Discipline & Dismissal Procedure and Equality Policy.

Where individuals from partner organisations are involved and are acting on behalf of the School, they will also be expected to comply with the relevant policies.

10.11 Data Protection

The Data Protection Act 2018, updates the 1998 Act and incorporates the General Data Protection Regulations (GDPR). It prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to email in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, the school respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, the school has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles

contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998 as updated by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR).

In order to comply with its duties under the Human Rights Act 1998, the school is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the school's wider business interests. In drawing up and operating this policy the school recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of the school's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998 as updated by the Data Protection Act 2018 and the General Data Protection Regulations (GDPR), associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

11. Remote Learning

There may be situations during the school year when learners may need to access remote learning. Systems and protocols are in place to help keep learners and teachers safe during remote education.

The following guidelines are expected of learners and must be adhered to;

- School uniforms must be worn for all remote learning sessions
- Learners must be in a suitable area of the home where they can be supervised. They should not be in their bedroom
- The same respect code used in school applies for these sessions. Failure to adhere to this will result in learners being removed from the session with a follow up consequence
- Any still images, video or audio from the session must not be used for a purpose for which it was not originally intended
- Strictly no phones to be present for the sessions

Cameras and microphones: At the start of each session all learners should have their cameras and microphones turned on. It will then be at the teacher's discretion as to whether microphones need to be muted and cameras turned off for the remainder of the learning session, and learners will be told this directly by the class teacher.

Recording of sessions: The school will not record any of the live engagement in learning for class learning sessions. However, if the school felt there was a need to do this, for example to monitor the quality of teaching for remote learning, then parents/carers would be informed.

For safeguarding purposes, virtual 1:1 sessions are recorded. The recordings are stored in a secure area and are only accessed in the event that a safeguarding concern is raised and are deleted after 30 days. Consent would be requested from parents/carers to take part in 1-1 sessions and if consent was not granted to agree to the sessions being recorded then the provision could not be offered to the learner.

Learners are not allowed to record any part of their learning session and/or edit any part of a pre-recorded learning session. No individual has the rights/permissions to share and/or edit footage from these sessions via social media, messaging or any other platform. If any learner is found to have done this, they will be prevented from accessing any further live or pre-recorded sessions and will be provided with alternative material to work from. Consequences will be implemented as appropriate and in line with the school's behaviour policy.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, staff meetings and bespoke cyber security training provided by Usecure).

The Designated Safeguarding Lead and Senior Leaders will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues on a bi-annual basis. This will form part of their annual safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

13. Monitoring arrangements

The School and Governing Body will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring of use of Internet
- Surveys/questionnaires of learners and staff

- Logs of e-safety incidents

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 3 years by the Senior Leader responsible for wellbeing in conjunction with the Designated Safeguarding Lead, the Senior Leader responsible for behaviour, Network Manager, the Subject Leader for PSHE and Subject Leader for Computer Science/IDEA. At every review, the policy will be shared with the Governing Body.

14. Complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Trust can accept liability for material accessed, or any consequences of Internet access.

The Deputy Headteacher is responsible for Wellbeing/E-Safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Behaviour Policy. Complaints related to child protection are dealt with in accordance with School/Local Authority child protection procedures.

15. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- RSE Policy
- PSHE Policy
- Staff disciplinary procedures
- Data Protection Policy and Privacy Notices
- Complaints procedure

This policy applies to all members of the Honywood School community (including staff, learners, volunteers, governors, parents/carers, visitors, community users) who have access to and are users of Honywood ICT systems, both in and out of the school premises.

Appendix 1

Internet Permission

As part of the school's ICT programme we offer learners supervised access to the Internet. Before being allowed to use the Internet all learners must obtain parental permission and both they and you must sign and return the iPad Acceptable Usage form as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet will enable learners to explore thousands of libraries, databases and bulletin boards that can support learners' learning across the curriculum. However, families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, learners may find ways to access other materials as well. We believe that the benefits to learners from access to the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages. However, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether to apply for access.

During school, teachers will guide learners toward appropriate materials. Outside school, families bear the same responsibility for such guidance with information sources such as television, telephones, movies, radio and other media.

Please find within this booklet a copy of the Guidelines for learners' Internet use which your child will be expected to follow if you agree to their use of the Internet. Once you have read the guidelines, please give or decline your permission for your child to use the Internet on the Summary of Consent section of the Admission form. In addition, please ask your child to sign their agreement to the guidelines.

Appendix 2

iPad Acceptable Use Policy (Version 5.2)

When we introduced iPads in September 2011 we were one of the first schools in the country to do so, since then many schools nationally have done the same. The purpose behind this decision was that we believe the device supports successful independent learning as well as creating authentic learning experiences for learners. One of the key factors in developing successful independent learners is to guide and support them in how they interact with their iPad. We use a range of media to communicate this such as the Honywood Headlines, school assemblies and through bespoke Learning Session 5 programmes.

We expect all learners to be safe and responsible when using technology whether it is their iPad, PCs in school or their own mobile technology. We believe it is essential that learners are aware of e-safety and know how to stay safe when using any new technology. If a learner has a mobile phone they must be very careful how they sync it with other devices especially with their school iPad. We will continue in school to address online safety and communicate with learners how to remain safe in the digital world in which we live.

All learners are responsible for looking after their iPad and need to appreciate that they must look after it as though it was their own so that when they eventually leave Honywood the iPad can be used by other learners in the school.

1. This document outlines the permitted use of Honywood loan iPads. All guidelines must be followed. Breaching these guidelines may result in disciplinary action and forfeit of the device.
2. All iPads, including accessories, remain the property of Honywood School and are on loan to learners whilst they are on roll.
3. All learners must bring their iPad to school every day unless they are not permitted on a school trip. Should a learner fail to bring their iPad in for five consecutive days, a colleague from the school will make a visit to the home to collect it.
    a. The iPad must be presented on request
    b. The iPad must be returned to the IT team upon the learner leaving school be that at the end of Cohort 11 or due to changing school.
    c. The school reserves the right to collect in any device immediately should it feel the need to do so.
    d. Failure to return the iPad and its accessories will result in us asking for a financial contribution for any items not returned.
4. All devices are collected by the IT team prior to the end of the summer term for essential maintenance and audit requirements.
5. Learners are not permitted to accessorise their loan iPad case in any way.
6. All learners are reminded that if they wish to use their loan iPad to store sensitive information they should only do so when this is essential and this remains the responsibility of the individual.
7. All iPads are configured to use the school Wi-Fi network where they are subject to robust filtering. Learners are permitted to configure their home Wi-Fi network however filtering in this instance will be regulated by their personal Wi-Fi supplier and parent/carer. We also utilise a web browser called Netsweeper, which offers some additional filtering while off site, but should be used in conjunction with your home provision.

8. Only official Apple iOS updates are permitted.
9. Software deployed by the school to the iPad **must not be removed or altered** in any way. All iPads are supervised and managed by our Mobile Device Management system (Meraki). You are not permitted to circumvent any of the iPad in-built security measures.
10. It is the learner's responsibility to back-up the device regularly using the guides supplied by the IT Team in the App on their iPad called **iPad back-up -** our advice is to store everything in Google Drive.
11. If there is a need to use an Apple ID on devices, only the Apple ID supplied by the school is to be used on the loan iPad. The Apple ID and password must not be shared with anyone. Using multiple Apple IDs may result in the device being locked by Apple for 90 days.
12. The sharing of Apps by using other people's Apple IDs is not permitted.
13. The use of illegally obtained software, that is all software that has not been validly purchased via the App Store, is not permitted.
14. Should parents/carers choose to add payment details to an iTunes account any costs incurred remain the responsibility of the family or individuals involved.
15. Only the Honywood IT Team are permitted to apply restriction codes to the device. Should a family want a restriction placed on the device please contact the IT team directly and they will be able to assist.
16. The loan iPad must not be subjected to a 'Jailbreak' method in order to install uncertified apps. Any attempted 'Jailbreak' could result in total loss of data and the inability of the school to provide support and the iPad will be confiscated from the learner.
17. Use of the iPad for questionable activity including the deliberate viewing of inappropriate material via the internet is not permitted and a consequence will be put in place should this occur.
18. Learners are not to undertake activities that contravene the Computer Misuse Act or Malicious Communications Act.
19. Learners must show due diligence in regard to the security of their loaned iPad at all times. This includes times when they are not using the device.
20. Only specific applications are permitted on the Honywood iPads. The list of apps available can be found on the Honywood iPad in the folder "Other Apps → Meraki MDM → Apps" .
21. Should a user run out of memory space on their loaned device, school content will take precedence over personal content.
22. Should your iPad, case or charger (and cable) be damaged or stolen you may have to fund the replacement or make a contribution to cover the cost of the repair as all users must return a fully functioning iPad and accessories provided at the end of their time at Honywood.
23. The taking of photographs or video recordings is only permitted where consent has been obtained.
24. When in a learning session, users should only engage with those apps that support their learning. Consequences will apply for any learners using their iPads inappropriately during or outside of learning sessions. The iPad may in some instances be removed for a period of time and/or some functions disabled. Where this is the case, paper based learning will be provided.
25. Should your iPad stop working in any way, or be damaged or stolen you must inform the IT team immediately and not attempt any repairs either yourself or through any other means. This includes any damage to the glass screen protector and case. The iPad must not be reset by anyone other than the IT department.
26. The iPad should never be used in Airplane Mode within the school.

27. Charging of the device is the responsibility of the learner apart from those who have requested that their device remain in school.
28. iPads must remain in the protective case supplied by the school at all times. This includes the front cover and glass screen protector. Any damage or graffiti to the case may result in the learner having to fund a new case and consequences to the learner.
29. Any educational apps downloaded to the iPad by the IT team must not be deleted from the device.
30. Learners may only use a number lock code on their device and are not permitted to use the fingerprint lock facility.

Appendix 3

Guidelines for Learners' Internet Access

1. Learners should keep all personal details secret – this includes passwords. Learners are responsible for any misuse of their password.

2. Use of the computer network and the Internet shall be for educational purposes only.

3. School staff may access any file held on any computer storage system or media that is part of or connected to the school network. The school reserves the right to access any storage media or other media brought into school and to monitor all communications. Learners should thus be aware that their files will not always be private.

The following are not permitted:

1. Sending or displaying offensive messages or pictures

2. Using obscene language

3. Using electronic mail to harass, insult or otherwise annoy others

4. Using other people's passwords

5. Accessing any other person's work or files without permission

6. Malicious damage to computers, software and other hardware

7. Violating copyright laws

8. Intentionally wasting limited resources

9. Game playing on the network

10. Downloading games or videos through the Internet

Consequences

Violation of the above rules may result in one of these sanctions:

1. Temporary or permanent ban on use of the Internet and electronic mail

2. Additional disciplinary action in line with the school's Behaviour Policy

3. When applicable, police or local authorities may be involved

Appendix 4

Internet Policy

The Internet provides access to a greater library of resources than could ever be provided by the school. However, whereas the resources in school are carefully selected to be consistent with national and school policies, those on the Internet are not. Apart from the educational resources that the Internet provides, there is also material of a potentially offensive nature, such as pornography, racist and fascist material. However, at Honywood we believe that learners should have the opportunity to use the vast range of resources on the Internet to support their learning and therefore learners will be able to access the Internet.

- The school will only consent to the Internet through a service provider that will employ measures making access to undesirable material difficult. It is acknowledged that there is too much material for the filter service to be fully effective
- The school will take appropriate action against anyone attempting to or succeeding in accessing such materials using school facilities
- The school will therefore reserve the right to electronically search all learners' folders and work stored on school ICT equipment and any media brought into school by learners
- Parental permission will be sought for each child before they access the Internet or electronic mail
- The Summary of Consent will be filed in each learner's record. Each class teacher will keep a record of learners who are entitled to use the Internet and electronic mail and any who are not
- Teachers will regularly remind learners of the rules governing Internet and electronic mail use
- The Network Manager will also regularly review the effectiveness of measures to restrict access to undesirable materials on the Internet
- E Safety Coordinator will provide guidance to teachers and learners on their use of the Internet and electronic mail
- The Network Manager supports the development of homepages and resource listings, liaising with other curriculum coordinators. This should help to guide learners towards resources, which are appropriate for their age range and ability
- Where learners are given freedom to search the Internet for information then the teacher should give clear learning objectives
- The Network Manager will review this policy in consultation with the Senior Management Team on an annual basis.

Appendix 5

Read receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment formats	When attaching a file, it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
E-mail address groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header/ subject	Convey as much information as possible within the size limitation. This will help those who get a lot of emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.

Absent	If you have your own email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of emails could be used in support, or in defence, of the School's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the e-mail can result in legally binding contracts being put into place.
Distribution lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using a reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	E-mail in the right context; care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the excessive use of capitals. It can be interpreted as shouting so consider how the style of your email may be interpreted by its recipient.
Forwarding e-mails	Consideration should be given when forwarding emails. They may contain information that you should consult with the originator before passing to someone else.

Large emails	For larger e-mails, particularly Internet emails, where possible send at the end of the day as they may cause queues to form and slow other people's e-mail.