Helsby High School

ICT and E-Mail Usage Policies and Procedures

This Document contains the following Policies and Procedures:

ICT Policy – Our Commitment

1. Helsby High School recognises that ICT has a very significant impact on all aspects of our modern society and that young people leaving school now require considerable ICT knowledge, skills and awareness if they are to be successful in their futures.
2. The school encourages safe use of ICT as a powerful learning tool to help enhance learning and teaching across the whole curriculum.
3. The school strives to provide staff and students with safe and appropriate access to ICT technology to support the education of students whilst at Helsby High School.
4. All staff shall be provided with appropriate support and training to ensure the benefits of ICT as a learning tool are maximised. The changing nature of ICT technology shall be reflected in staff development programmes.
5. The school has clear guidance on the appropriate use of ICT technology (including E-mail and internet access) at school.
6. Helsby High School is committed to providing a safe environment for students to use ICT technology (including E-mail and internet access). The school shall monitor use of ICT to ensure on-line safety principles are maintained.
7. Each member of the school knows their roles and responsibilities in the use of ICT technology at Helsby High School.
8. The ICT Policy is regularly reviewed, evaluated and updated.

Monitoring and Reviewing the Policy

This policy shall be reviewed on a periodic basis and reissued. Period for review shall not exceed 24 months.

E-mail Acceptable Use Procedure

1.0 Aim

The purpose of this procedure is to ensure that all e-mail sent from an e-mail account under the control of Helsby High School complies with acceptable standards for intent, content and appropriate recipients.

2.0 Scope

This procedure covers the safe and appropriate usage of e-mail accounts assigned to students, staff, governors and volunteers associated with Helsby High School. This applies to usage of e-mail sent from any e-mail address assigned by Helsby High School, whether sent from a computer or other electronic device, either from school premises or elsewhere.

This procedure does not, however, cover use of private e-mail accounts.

3.0 Definitions

E-mail	Electronically transmitted message sent via computer network and mobile devices.

4.0 Procedure

4.1 Roles and Responsibilities

4.1.1 The Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for ensuring that systems are maintained to monitor e-mail correspondence to ensure that this complies with the standards expected by Helsby High School and Local Authority. They shall ensure that appropriate security is enforced to prevent unauthorised access to the private correspondence of staff and students.

4.1.2 ICT Network Manager

It is the responsibility of the ICT Network Manager to monitor appropriate use of the system.

4.1.3 All E-mail Account Holders

It is the responsibility of all e-mail account holders (students, teaching and support staff employed at Helsby High School, and volunteers associated with Helsby High School) to read and understand the relevant E-mail Acceptable Use Form to sign to indicate their agreement to abide by the principles therein. All emails, both internally and externally are encrypted unless the sender dictates that this communication is to be sent unencrypted.

4.2 Procedure

4.2.1 E-mail Acceptable Use Forms

All users of the Helsby High School e-mail system shall be expected to sign an agreement indicating their acceptance to operate within the guidelines set out for safe and appropriate e-mail use. These guidelines are set out in a series of acceptable use forms tailored for each user group.

- "E-mail Acceptable Use Form Years 7-13" shall be issued to all lower school students.

- E-mail acceptable use conditions for staff and governors forms part of "ICT Acceptable Use for Staff and Governors".

Each proposed user of the Helsby High School e-mail system must sign the relevant form to indicate their acceptance to abide by the conditions of use before they will be assigned an e-mail account.

The agreement shall last for the duration of an academic year, unless revoked as part of a disciplinary action.

Records of agreements to operate within E-mail Acceptable Use conditions as detailed in this section are to be held in the HR files.

4.2.2 Monitoring

Each format for the E-mail Acceptable Use agreement advises the user that e-mail use may be monitored to ensure acceptable standards of use are maintained.

The school may monitor e-mail of any user, either by automated or manual means, at any time. The privacy of the e-mail account holder must be maintained at all times and information gathered during monitoring activities must be considered as confidential.

E-mail accounts for students may be monitored by:

- All staff via the ICT Support team
- ICT Department via the RM Management console

E-mail accounts for staff and governors may be monitored by:

- Headteacher
- Leadership team member with responsibility for on-line safety
- ICT Network Manager

Please refer to "Administration of User Accounts" for appropriate response to discovery of e-mail usage which does not comply with this procedure.

4.3 Monitoring and Reviewing the Procedure

This procedure shall be reviewed on a periodic basis and reissued. Period for review shall not exceed 24 months.

ICT Acceptable Use Procedure for Staff, Governors and Volunteers

1.0 Aim

The purpose of this procedure is to advise staff, governors and volunteers associated with Helsby High School of if, when and under what conditions they may use the school's/Local Authority's communications and information systems for personal reasons. It sets standards to ensure that employees understand the position and do not inadvertently use communications and information in inappropriate circumstances.

The school recognises employees' rights to privacy but needs to balance this with the requirement on the school (as a public service) to act appropriately, with probity, to safeguard its business systems, and to be seen to be doing so.

In applying the policy, the school will act in accordance with the Human Rights Act 1998 and other relevant legislation and will recognise the need of employees to maintain work/life balance.

2.0 Scope

This procedure covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, for example:

- mail systems (internal and external)
- internet and intranet (e-mail, web access and video conferencing)
- telephones (hard wired and mobile)
- cameras and image capturing devices
- fax equipment
- computers – this covers ANY computer used for work purposes, whether at the place of work or elsewhere (see Annex on Laptops For Teachers)
- photocopying, printing and reproduction equipment
- recording / playback equipment
- documents and publications (any type or format)

The procedure applies to all employees (as a contractual term), agency staff and to other people acting in a similar capacity to an employee. It will also apply to staff of Contractors and other individuals providing services/support to the school (e.g. volunteers) and takes account of the requirements and expectations of all relevant legislation.

3.0 Definitions

E-mail	Electronically transmitted message sent via computer network and mobile devices.

4.0 Procedure

4.1 Roles and Responsibilities

4.1.1 The Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for ensuring that systems are maintained to monitor e-mail correspondence to ensure that this complies with the standards expected by Helsby High School and the Local Authority. They shall ensure that appropriate security is enforced to prevent unauthorised access to the private correspondence of staff and students.

4.1.2 ICT Network Manager

It is the responsibility of the ICT Network Manager to monitor appropriate use of the system.

4.1.3 All Staff, Governors and Volunteers

It is the responsibility of all staff, governors and volunteers associated with Helsby High School to read and understand this procedure and the accompanying ICT Acceptable Use Form and to sign to indicate their agreement to abide by the principles therein.

4.2 Procedure

4.2.1 Use of Equipment and Facilities

4.2.1.1 Use of Facilities

The school's Code of Conduct states that staff must not carry out personal activities during working hours, nor mix private business with official duties. Official equipment and materials should not be used for general private purposes without prior permission from the Headteacher or an appropriate line manager. This will usually be in writing or may be covered by the parameters agreed by the Headteacher/manager with the team.

4.2.1.2 Facilities for Private Use

The following are provided as examples to illustrate where it might be reasonable for permission to be given for reasonable use for private purposes, under the conditions shown and after getting prior approval, in writing if this is required. The Headteacher or a senior manager may veto private use at any time if they consider that circumstances justify this in general or particular cases, e.g. because of improper use or over-use. A charge may be made for materials if the values are significant.

- Social or recreational activities associated with school employment.
- Regular activity for a legitimate voluntary body or charity - but prior written approval from a senior manager must be obtained.
- Training or development associated with school employment.
- Occasional and brief essential family communications or other personal messages. In emergencies permission might need to be obtained retrospectively or again this may be covered by the general parameters agreed with the team.

If given permission, approved acceptable private use should normally take place in the employee's own time but where this is not practicable or sensible, any disruption to the employee's official work or that of colleagues must be minimal. Official work will always take precedence.

All uses, whether for private or official purposes, must observe:

- the law
- Financial Regulations and Codes of Practice on Financial Management
- Terms of employment, especially the Code of Conduct for Employees

It is not acceptable to use school equipment and materials or an employee's own equipment/materials in the workplace in any of the following contexts:

- Illegal activity.
- Activities for private gain.
- Radicalisation and extremism.
- Excessive personal messages.
- Playing games.*
- Gambling.
- Political comment or any campaigning.

- Personal communications to the media.
- Use of words or visual images that are offensive, distasteful or sexually explicit.
- Insulting, offensive malicious or defamatory messages or behaviour.
- Harassment or bullying.
- Random searching of the web.
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Using message encryption or anonymised web search, except where encryption is required for official Helsby High School business purposes.
- Racist, sexist or other conduct or messages which could embarrass the school or bring it into disrepute.

* except those games pre-loaded as part of the Microsoft programme suite, which may be accessed in the employee's own time.

4.2.2 ICT Acceptable Use

Staff, governors and volunteers must use school ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. They must recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. It is their responsibility to, where possible, educate the young people in their care in the safe use of ICT and embed on-line safety in their work with young people.

For professional and personal safety, staff, governors and volunteers must:

- understand that the school will monitor their use of the ICT systems, e-mail and other digital communications.
- understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, smart devices, e-mail, VLE etc.) out of school.
- understand that the school ICT systems are primarily intended for educational use and that they will only use the systems for personal or recreational use within the policies and procedures set down by Helsby High School.
- not disclose username or password to anyone else, nor will they try to use any other person's username and password.
- immediately report any illegal, inappropriate or harmful material or incident they become aware of to the On-line safety Coordinator/ICT Network Manager.

Staff, governors and volunteers should be professional in all communications and actions when using school ICT systems and must:

- not access, copy, remove or otherwise alter any other user's files, without their express permission.
- communicate with others in a professional manner, avoiding the use of aggressive or inappropriate language and appreciating that others may have different opinions.
- ensure that images of others are only taken/published with their permission and in accordance with the school's policy on the use of digital / video images. They must refrain from the use of personal equipment to record these images. Where these images are published (e.g. on the school website / VLE) it must not be possible to identify by full name, or other personal information, those who are featured.
- communicate with students and parents / carers using official school systems only, retaining a professional tone and manner, in line with our policies and procedures
- not engage in any on-line activity that may compromise professional

responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When using personal hand held / external devices (PERSONAL DEVICEs / laptops / mobile devices / USB devices etc.) in school, the rules set out in this document will apply in the same way as if school equipment was used. The school may set out additional rules which must also be followed, including ensuring that any such devices are protected by up to date anti-virus software and are free from viruses.
- Attachments to e-mails must not be opened, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Staff, governors and volunteers must ensure that data is regularly backed up, in accordance with relevant school policies.
- Staff, governors and volunteers must not attempt to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. They must not attempt to use any programmes or software that might allow bypassing of filtering / security systems in place to prevent access to such materials.
- Staff, governors and volunteers must not attempt to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. Such data transfers can only be attempted with prior permission from the ICT Network Manager.
- Staff, governors and volunteers must not install or attempt to install programmes of any type on a machine, or store programmes on a computer, or try to alter computer settings, unless authorised to do so.
- Staff, governors and volunteers must not disable or cause any damage to school equipment, or the equipment belonging to others.
- Staff, governors and volunteers must only transport, hold, disclose or share personal information about themselves or others, as outlined in the schools Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- Student and staff data must be kept private and confidential, in line with the data protection policy, except when it is deemed necessary that it is required by law or by school policy to disclose such information to an appropriate authority.
- Staff, governors and volunteers must immediately report any damage or faults involving equipment or software, however this may have happened, to the ICT support team.

When using the internet in a professional capacity or for school sanctioned personal use, staff, governors and volunteers must:

- ensure that permission has been sought to use the original work of others in their own work
- refrain from downloading or distributing copies (including music and videos), where material is protected by copyright

4.2.3 E-mail Acceptable Use

Use of e-mail by staff of Helsby High School is permitted and encouraged where such use supports the goals and objectives of the School. However, Helsby High School has a policy for the use of e-mail whereby the staff, governors and volunteers must ensure that they:

- Do not send sensitive data (under data protection and child protection) to

unauthorised users and not outside the school network – e-mail is an unsecure communication;
- All communications should follow the agreed School procedures, as is the case with letters, only DL, YL/KSL or SLT should be sending E-mail direct to parents;
- All e-mails sent should be written in a formal style and should address parents using their title and surname;

Use e-mail in an acceptable way;

- Do not create unnecessary risk to the School by their misuse of the internet;
- Comply with current legislation;
- Be aware that e-mails to students should only be sent to the designated school e-mail account for that student. Staff should not send e-mails to a student's private e-mail account;
- Be aware that e-mail communications between staff and students should be of a professional nature.

The following is considered as unacceptable behaviour:

- use of personal communications systems (e.g. a personal e-mail address) for School use of any description
- use of School communications systems for personal use or sending chain letters
- distributing, accessing or storing images, text or materials that might be considered indecent, inappropriate, pornographic, obscene or illegal
- distributing, accessing or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying
- accessing copyrighted information in a way that violates the copyright law
- breaking into the School's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-School related matters
- transmitting unsolicited commercial or advertising material (SPAM)
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the school network
- accessing another person's e-mail account
- sharing their password with another person
- e-mailing a student via the student's private e-mail address. All students have a school e-mail account.

4.2.4 Inadvertent Access to Inappropriate Sites and Inappropriate E-mails

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify their school/manager and ICT support of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

Employees may find themselves receiving e-mails which contravene this policy. In the case of comparatively innocuous material (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the school's/Local Authorities' policy. If there is repetition, the employee should retain the messages and notify their Headteacher/line manager. If the e-mails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the Headteacher/line manager notified immediately. Employees should notify the

sender that they do not wish to receive such material and keep a record of doing so.

4.2.5 ICT Acceptable Use Forms

All staff, governors and volunteers associated with Helsby High School shall be expected to sign an agreement indicating their acceptance to operate within the guidelines set out within this procedure for safe and appropriate ICT use. These guidelines are set out in a series of acceptable use forms tailored for each user group.

Each proposed user of the Helsby High School e-mail system must sign the relevant form to indicate their acceptance to abide by the conditions of use before they will be assigned a user account.

The agreement shall last for the duration of an academic year, unless revoked as part of a disciplinary action.

Signed copies of the ICT Acceptable Use and E-mail Policy as detailed in this section are to be held in HR records.

4.2.6 Monitoring

The school may monitor user accounts of any staff or volunteers associated with Helsby High School, either by automated or manual means, at any time. All employees should be made aware at induction, at intervals thereafter and possibly through automatic messages on school equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using school equipment provided for official/ work purposes, and that the school reserves the right to monitor all communications including their content. This monitoring is carried out to ensure that equipment and systems are used efficiently and effectively, to maintain the system's security and to detect any breaches of this policy or the law.

The privacy of the user account holder must be maintained at all times and information garnered during monitoring activities must be considered as confidential. Monitoring information will not be accessible (or distributed) any more widely than is necessary for the purposes for which it is needed.

Please refer to "Administration of User Accounts" for appropriate response to discovery of e-mail usage which does not comply with this procedure.

4.2.6.1 Telephones and Fax

The school reserves the right to monitor communication content selectively if abuse is suggested. However, such monitoring would only take place following an assessment that such steps are necessary to further a particular investigation or concern. It would only be authorised following the advice of the Headteacher. Where calls are made via the school an automatic record is kept of every number called, from where and the duration of the call. Further action is taken where particular numbers called or the frequency and duration of calls suggest abuse of this policy.

4.2.6.2 E-mail

Helsby High School accepts that the use of e-mail is a valuable School tool. However, misuse of this facility can have a negative impact upon staff productivity, the reputation of the School and potentially bring harm to vulnerable people.

In addition, all of the School's e-mail resources are provided for School purposes. Therefore, the School maintains the right to examine any systems and inspect any data recorded in those systems.

In order to ensure compliance with this policy, the School will use monitoring software in order to check upon the use and content of e-mails periodically. When using Helsby High School's network, every incoming and outgoing e-mail message is automatically swept for key words which could indicate misuse. The school reserves the right to apply similar screening to its own e-mail systems. Such monitoring is for legitimate purposes only. The use of the network and School assigned e-mail accounts will be monitored and the school is able to see all e-mails and files on the School's system.

E-mail accounts for staff, governors and volunteers may be monitored by:

- Headteacher
- Leadership team member with responsibility for on-line safety
- ICT Network Manager

4.2.6.3 Internet Access

When using Helsby High School's network, access to some web sites is automatically prevented (e.g. pornographic, racist and violent sites) and others are restricted (e.g. MP3 music sites and Web Chat) and a message warns that these types of sites are blocked. An automatic record is, however, made of all sites visited and a sweep made of site names and content against pre-determined criteria, to identify inappropriate sites together with attempts made to access such sites. The school reserves the right to apply similar restrictions and screening to its own web access systems.

User accounts for staff, governors and volunteers may be monitored by:

- Headteacher
- Leadership team member with responsibility for on-line safety
- ICT Network Manager

4.2.6.4 Posted Mail

The privacy of internal and external postal communications marked 'personal' will normally be respected (unless abuse of this policy is suspected) but all other communications may be opened for good reason by the Headteacher, line manager, secretary or colleague.

4.2.6.5 Access to and Retention of Monitoring Information

Access to routine monitoring information at Helsby High School is restricted to the ICT support team. Regular reports will be produced identifying high usage of IT resources and areas of high risk (e.g. as a result of weak passwords or accessing inappropriate web content). These reports will be made available to ICT Network Manager. If a potential issue of abuse is identified the ICT Network Manager will be given access to more detailed information to enable them to decide whether further investigation is necessary and initiate appropriate action. The ICT Technicians and ICT Network Manager will respect the confidentiality of all communications and disclose the contents of communications only where there are grounds for suspecting abuse of this policy. Where this is the case, the School Business Manager and the Headteacher may then be involved and are likely to be made aware of the contents of communications.

4.2.7 CCTV surveillance

Permanently fitted surveillance cameras are installed by the school only for security and safety reasons and will always be visible to people within their range. Video

recording will be kept secure, the information used only for security purposes. No automatic connections will be made between information from security cameras and other monitoring sources.

Covert monitoring will only be used in connection with a criminal investigation or where there is suspected abuse of terms of employment, e.g. the sickness scheme, is being investigated. This will always be in accordance with the statutory safeguards applicable to such activity and only authorised following careful consideration of the need for such action.

The school uses CCTV surveillance cameras to monitor the school site at all times. These are used to help protect the school site from intruders.

4.2.8 Security

Every employee must observe the school's communications and information technology security requirements and act responsibly when using equipment and materials. Employees will be provided with the necessary briefing and training to enable them to comply with this requirement.

The Headteacher will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of records or systems. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take, action within their authorised power to safeguard, report, to the Designated Safeguarding lead and/or ICT Network Manager and, if possible, resolve the situation (e.g. disconnect any infected machine from the network (remove the cable) and notify the ICT Network Manager).

4.2.8.1 Reporting Misuse

If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to the Headteacher or a senior manager or use the Whistleblowing Policy.

4.3 Consequences of Breach of Procedure

If a member of staff is found to have breached this policy, they will face the instant withdrawal of their e-mail account and/or network usage for an indefinite period.

This will be subject to review by SLT who will be notified of any breach of this policy.

If a breach of this policy is deemed to have breached the school's Safeguarding Policy, the Allegations of Abuse Against a Member of Staff policy will be followed.

Breaches of this policy may result in the application of the Disciplinary Procedure and may, if deemed sufficiently serious, be treated as gross misconduct. In the case of contractors, agency staff, volunteers or partnership employees, breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

4.4 Agreement

All staff, governors and volunteers who have been granted the right to use the school's ICT services are required to sign this agreement confirming their understanding and acceptance of this policy.

This agreement will last for the duration of the academic year.

5.0 Monitoring and Reviewing the Procedure

This procedure shall be reviewed on a periodic basis and reissued. Period for review shall not exceed 12 months.

6.0 Supporting Documentation

ICT Acceptable Use Form for Staff, Governors and Volunteers

Administration of User Accounts Procedure

1.0 Aim

The purpose of this procedure is to ensure that students, staff, governors and volunteers are able to safely and appropriately access ICT facilities at Helsby High School.

2.0 Scope

This procedure covers the safe and appropriate usage of user accounts assigned to students, staff, governors and volunteers associated with Helsby High School. This applies to access to software packages and servers managed by Helsby High School.

This procedure does not, however, cover use of school network (Wired or wifi) infrastructure. It also does not cover specific usage of E-mail accounts managed by Helsby High School.

3.0 Definitions

E-mail	Electronically transmitted message sent via computer network
YL	Year Leader
KSL	Key Stage Leader
DL	Department Leader
ICT	Information Communication and Technology
SLT	Senior Leadership Team

4.0 Procedure

4.1 Roles and Responsibilities

4.1.1 The Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team are responsible for ensuring that systems are maintained to support this procedure. They shall ensure that appropriate security is enforced to prevent unauthorised access to the private correspondence of staff and students.

4.1.2 ICT Network Manager

It is the responsibility of the ICT Network Manager to monitor appropriate use of the system.

4.1.3 All User Account Holders

It is the responsibility of all user account holders (students, teaching and support staff employed at Helsby High School, governors and volunteers associated with Helsby High School) to appropriately protect access to their personal accounts. Users should not provide access to this account to other users without express permission from the ICT Network Manager. Providing unauthorised access to an account can lead to the breach of GDPR 2018, Child Protection and Copyright Legislation and as such is to be considered hacking.

4.2 Procedure

4.2.1 User Account Assignment

All staff, students, governors and, where appropriate, volunteers associated with Helsby High School, shall be assigned a user account for their personal use in relation to their activities at Helsby High School.

The user account will permit the following:

- Access to software and internet services managed by the school
- Access to a unique e-mail address to be used in activities associated with the school. The e-mail address shall have the format [NAME]@helsbyhigh.org for students, and staff [NAME]@helsbyhigh.org.uk where [NAME] shall be a unique identifier assigned by the school.
- Access to data storage servers managed by Helsby High School, such as Portico. Access should be tailored to permit access solely to drives relevant to the activities of that user, but should include access to a personal drive space to allow storage of personal files or work related to their activities at school.

4.2.2 User Accounts

The user account remains the property of the school and as such the school reserves the right to investigate and monitor the account at any time.

As server capacity is limited, the user accounts should not be used for personal use such as personal pictures, music and videos. This also includes storage on laptops and smart devices.

The user accounts are used to control access to data on the network. As a default, all users are provided with the minimum amount of access deemed necessary to perform their expected day to day activities. Any additional permission to other resources is to be requested by the DL, who should forward these requests to the ICT Network Manager.

Any problems which develop with a user account (such as forgotten passwords or other user account settings needing to be reset) should be directed to the ICT Support team. A problem with a user account is not a reason to use another user's account.

4.2.3 Passwords

4.2.3.1 Students

All students are issued a password which is generated by the ICT Support team. This password is distributed to students in Year 7 by the Computing Department.

If a student has forgotten their password or suspects that someone else has gained access to their account, the ICT Support team can reset their password. Students are instructed about the correct use of their passwords as part of "Year 7 Introduction" a unit delivered by the Computing Department at the start of Year 7.

Any attempt to gain access to another user's account, or deliberate sharing of the password with other users is considered unacceptable as it breaches any implemented security systems. As such any access unauthorised by the ICT Network Manager is considered hacking. It is the user's responsibility to monitor their own account and in the case hacking, they should notify the ICT Network Manager as soon as suspicion has been raised. If the user is aware of an unauthorised access, but does not notify the ICT Network Manager, then that user will also be considered as hacking the network.

4.2.3.2 Staff, Governors and Volunteers

Staff accounts have access to a number of sensitive resources such as RMStaff, Office and SIMS. Staff passwords should never be shared and

members of staff should never allow a student to use their account under any circumstances.

To help secure the staff accounts, staff are allowed to set their own passwords. However, the school network will automatically enforce a minimum requirement on that password, as listed below.

Staff password structure (including SIMS):

- Minimum of 6 characters with a mix of upper and lower case with at least 1 number.
- Lifetime: 90 days or termly

Finance staff password structure:

- Minimum of 8 characters with a mix of upper and lower case with at least 1 number.
- Lifetime: 50 days or termly

System Administrators password structure:

- Minimum of 8 characters with a mix of upper and lowercase with at least 2 numbers.
- Lifetime: 50 days or termly

Computing Department password structure:

- Minimum of 7 characters with a mix of upper and lower case with at least 2 numbers.
- Lifetime: 90 days or termly

4.2.4 Monitoring

The school may monitor the usage of any user account, either by automated or manual means, at any time. The privacy of the user account holder must be maintained at all times and information garnered during monitoring activities must be considered as confidential.

User accounts for students may be monitored by:

- All staff via the ICT Support team
-

User accounts for staff, governors and volunteers may be monitored by:

- The Headteacher
- Leadership team member with responsibility for on-line safety
- ICT Network Manager

4.2.5 Inappropriate Usage of User Account

4.2.5.1 Inappropriate Usage by Student

In the event of a breach of E-mail Acceptable Use or breach of security such as a student logging on as another (either shared or hacked) to access the internet, rename/move work, install games etc. The teacher identifying this breach must notify the ICT Network Manager who will investigate and where necessary arrange for a letter to be sent home and remove the student's access rights for a period of time.

4.2.5.2 Inappropriate Usage by Staff, Governor or Volunteer

Due to the sensitive nature of the data accessible, a breach in password security is to be considered very seriously. If the staff, governors or volunteers are made aware of a possible password breach they must immediately:

- Change their password. If this cannot be done, then inform the ICT Network Manager who can do this on the staff members behalf
- Inform the ICT Network Manager of this breach and any suspicions the staff member may have; such reporting is covered by the school's Whistleblowing Policy

Any deliberate delay in contacting the ICT Network Manager will result in the user account being suspended and the matter being passed to SLT. The staff members DL will also be informed.
If the ICT Network Manager is made aware of a staff account being breached they will suspend the account immediately and inform the staff member directly. The DL will also be notified. The staff member can then arrange for a new password with the ICT Network Manager.
If staff are found to be using their account in contravention of Procedure 2.2 "ICT Acceptable Use Agreement for Staff, Governors and Volunteers", this will result in the account being suspended and the matter being passed to SLT. The staff members DL will also be informed.

4.3 Monitoring and Reviewing the Procedure

This procedure shall be reviewed on a periodic basis and reissued. Period for review shall not exceed 12 months.

5.0 Supporting Documentation

None Required

On-line Safety Procedure

1.0 Aim

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

On-line safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children and young people.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Schools must be aware that students and staff cannot be completely prevented from being exposed to risks both on and off-line. Students should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good on-line safety practice in the classroom in order to educate and protect the students in their care. Members of staff also need to be informed about how to manage their own professional reputation on-line and demonstrate appropriate on-line behaviours compatible with their role.

Breaches of an on-line safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider school community. It is crucial that all users in the setting are aware of the consequences that on-line actions can have.

Schools must be aware of their legal obligations to safeguard and protect students on and off-line and the accountability of these decisions will sit with the Headteacher and the Governing body.

The on-line safety policy is essential in setting out how the school plans to develop and establish its on-line safety approach and to identify core principles which all members of the school community need to be aware of and understand.

2.0 Scope

This procedure covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use, where students may be vulnerable to inappropriate material.

3.0 References

ICT Acceptable Use Students
ICT Acceptable Use Staff, Governors and Volunteers
Administration of User Accounts

4.0 Definitions

Cyberbullying	The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone

5.0 Procedure

5.1 Roles and Responsibilities

5.1.1 The Headteacher and Senior Leadership Team

The Headteacher and Senior Leadership Team have a legal responsibility to safeguard students and staff and this includes on-line activity.

It is the Senior Leadership Team's responsibility to ensure appropriate procedures are in place and all members of staff are suitably trained to supervise Internet access.

5.1.2 On-line Safety Co-ordinator and ICT Network Manager

It is the responsibility of the On-line Safety Co-ordinator and ICT Network Manager to administer this procedure and to monitor appropriate use of the system.

5.2 Procedure

5.2.1 Security of Network Systems

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
- Personal data sent over the Internet or taken off site should be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to e-mail.
- Files held on the school's network will be regularly checked using Securus which e-mails concerns to ICT support.
- The ICT Network Manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

5.2.2 E-mail Security

E-mail is an essential means of communication for both staff and students. Directed e-mail use can bring significant educational benefits.

Restriction of incoming and outgoing e-mail to approved addresses and filtering for unsuitable content is carried out.

In the school context, e-mail should not be considered private and Helsby High School reserves the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided e-mail account to communicate with parents/carers, students and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Students may only use approved e-mail accounts for school purposes.
- Students must immediately tell a designated member of staff if they receive offensive e-mail.

- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from a member of staff or parent.
- Staff will only use official school provided e-mail accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal e-mail accounts may be blocked.
- E-mails should be processed in the same way as letters when sent externally. They should be written carefully by DL/YL/KSL and authorised by SLT as appropriate
- The forwarding of chain messages is not permitted.
- Schools will have a dedicated e-mail for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal e-mail accounts during school hours or for professional purposes.

This forms the basis of Procedures 2.1 "ICT Acceptable Use Students" and 2.2 "ICT Acceptable Use for Staff, Governors and Volunteers".

5.2.3 Published Content

- The contact details on the website should be the school address, e-mail and telephone number. Staff or students' personal information must not be published.
- E-mail addresses will be published carefully on-line, to avoid being harvested for spam.
- The Headteacher will take overall editorial responsibility for on-line content published by the school and will ensure that content published is accurate and appropriate.
- The school website will be checked by SLT for compliance with intellectual property rights, safeguarding and copyright legislation.

5.2.3.1 Publishing of Students' Images or Work

Still and moving images and sound add liveliness and interest to a publication, particularly when students can be included. Nevertheless, the security of staff and students is paramount. Although common in newspapers, the publishing of students' names with their images is not acceptable. Published images could be reused, particularly if large images of individual students are shown. Students in photographs should, of course, be appropriately clothed.

- Images or videos that include students will be selected carefully and will not provide material that could be reused.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of students are electronically published.
- Students' work can only be published with their permission or the parents.
- Written consent will be kept by the school where students' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of students which outlines policies and procedures.
- Students need to be taught the reasons for caution in publishing personal information and images on-line as it may compromise their safety.

5.2.4 Social Networking, Social Media and Personal Publishing

Social networking includes activities conducted on-line outside working hours such as blogging (writing personal journals to internet pages which are publicly accessible), involvement in social networking sites such as Facebook, Myspace, Bebo, personal publishing tools including blogs, wikis, forums, bulletin boards, multiplayer on-line gaming, chatrooms, instant messenger and many others. Posting material, images or comments on sites such as You Tube, can have a negative effect on the reputation or image of the school. In addition, Helsby High School has a firm commitment to safeguarding students in all aspects of its work.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer on-line gaming, chatrooms, instant messenger and many others.

- Every member of staff, governor, or volunteer has a responsibility to ensure that they protect the reputation of the school and to treat colleagues and members of the school with professionalism and respect.
- It is important to protect every member of staff, governor or volunteer at Helsby High School from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding students is a key responsibility for all members of staff, governors and volunteers and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. No-one who works in the school either as a paid employee or volunteer must communicate with students via social networking (except through Moodle). If this is a requirement of another professional role outside of school (e.g. Scouting, Guiding) then staff should notify the relevant DL or YL/KSL and this will subsequently be recorded by HR on their personnel file.
- Blogging and accessing social networking sites at work using school equipment is not permitted.
- No communications relating to any specific event, protocol, student or person at Helsby High School should be shared, irrespective of their anonymity.
- The School will control access to social media and social networking sites.
- Staff official blogs or wikis should be run from the school website with approval from the Senior Leadership Team. Members of staff are strongly advised not to run social network spaces for student use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy on-line and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

5.2.5 Filtering Management and Access Profiles

Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the school community. Older students, as part of a supervised project, might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs,

medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled garden or "Whitelist" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of content.
- Dynamic content filtering examines web page content or e-mail for unsuitable words.
- Keyword lists filter search engine searches and URLs for inappropriate results and web addresses. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject rated pages exceeding a threshold.
- URL monitoring records the Internet sites visited by individual users. Reports can be produced to investigate student access.

It is important that staff recognise that filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. mobile phone).

Occasionally, mistakes may happen and inappropriate content may be accessed. It is therefore important that students are taught to report such incidents so that this content may be blocked to prevent future access.

In addition, Internet Safety Rules should be displayed, and both students and adults should be educated about the risks on-line. There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Such incidents are reported to parents where appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as the Police or CEOP.

Websites which schools believe should be blocked centrally should be reported to the Local Authority. Staff should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of students.
- The school will report breaches of filtering. All members of the school community (all staff and all students) will be aware of this.
- If staff or students discover unsuitable sites, the URL will be reported to the School On-line Safety Coordinator and ICT Network Manager who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as the Police or CEOP.

5.2.6 Personal Data

The quantity and variety of data held on students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The GDPR 2018 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the GDPR 2018, every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
The GDPR of 2018 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Regulations sets standards which must be satisfied when processing personal data (information that will identify a living individual). The Regulation also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with the individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

5.2.7 Video Conferencing

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education. Equipment ranges from small PC systems (web cameras) to large room-based systems that can be used for whole classes or lectures.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment will not be taken off school premises without permission.

5.2.7.1 Protection of Users

- Students will ask permission from a teacher before making or answering a videoconference call.
- Videoconferencing will be supervised by a member of staff and appropriate for the students' age and ability.
- Parents and carers consent should be obtained prior to students taking part in videoconferences.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.

5.2.7.2 Control of Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of the videoconference should be

made clear to all parties at the start of the conference. Recorded material shall be stored securely.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for your class.

5.2.8 Use of Personal Devices

Mobile phones and other personal devices such as Games Consoles, Tablets, PERSONAL DEVICEs and MP3 Players etc. are considered to be an everyday item in today's society to get on-line regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile phones can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged;
- Their use can render students or staff subject to cyberbullying;
- Internet access on phones and personal devices can allow students to bypass school security settings and filtering.
- They can undermine classroom discipline as they can be used on "silent" mode;
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff.

Due to the widespread use of personal devices it is essential that the school takes steps to ensure mobile phones and devices are used responsibly. It is essential that student use of mobile phones does not impede teaching, learning and good order in classrooms. Staff should be given clear boundaries on professional use.

- The use of mobile phones and other personal devices by students and staff in school are covered in the school Acceptable Use or Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the student or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with prior consent from the Senior Leadership Team.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought into school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

5.2.8.1 Students' Use of Personal Devices

- If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to students or parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

5.2.8.2 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside the setting in a professional capacity, unless in case of an emergency and only after permission has first been sought from the Senior Leadership Team.
- Staff will be issued with a school phone where contact with students or parents/carers is required such as on a school trip.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team and in emergency circumstances.
- Personal mobile phones /smart devices should not be accessible or in view of students during the school day.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose, having sought permission from the Senior Leadership Team.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Cyberbullying

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming devices or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst students. These measures should be part of the school's behaviour policy which must be communicated to all students, school staff and parents
- Gives Headteachers the ability to ensure that students behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as on-line or via text) is reported to the school, it should be investigated and acted on within reason.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feel that an offence may have been committed they should seek assistance from the Police.

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying as part of the Anti-bullying Policy (part of the On-line safety policy 1.4.5).
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's on-line safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully being asked to remove any material deemed to be inappropriate or contacting a service provider to remove content if the bully refuses or is unable to delete content.
- Internet access being suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Informing parent/carers of students.
- Contacting the Police if a criminal offence is suspected.

5.2.9 Use of Learning Platforms (Moodle)

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students and parents, as well as support for

management and administration. It can enable students and teachers to collaborate in and across schools, sharing resources and tools for a range of topics. It also enables the creation and management of digital content and students can develop on-line and secure e-portfolios to showcase examples of work.

The Learning Platform at Helsby is referred to as Moodle or the Virtual Learning Environment, VLE. As usage grows throughout the school then more issues could arise regarding content, inappropriate use and behaviour on-line by users. The Senior Leadership Team has a duty to annually review and update the policy regarding the use of the Learning Platform, and all users must be informed of any changes made.

- Only members of the current student body, parent/carers and staff community will have access to Moodle.
- All users will be mindful of copyright issues and will only upload appropriate content to Moodle.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns about content on Moodle may be recorded and dealt with in the following ways:
    a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    b) The material will be removed by the site administrator if the user does not comply.
    c) Access to Moodle for the user may be suspended or restricted.
    d) The user will need to discuss the issues with a member of the Senior Leadership Team before reinstatement.
    e) A student's parent/carer may be informed.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

5.2.10 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual on-line classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, on-line learning and parental access are becoming embedded within school systems. On-line communities can also be one way of encouraging a disaffected student to keep in touch.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal device with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a student using a phone to video a teacher's reaction in a difficult situation.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many students and families; this could be used to communicate a student's absence

or send reminders for exam coursework. There are dangers for staff however if personal phones are used to contact students and therefore a school owned phone should be issued.

The inclusion of inappropriate language or images is difficult for staff to detect. Students may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's behaviour and/or anti-bullying policies.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy. This also includes the use of digital cameras and devices that take images such as an I-pad.

5.2.11 Granting of Internet Access

Normally most students will be granted Internet access. Parental permission should be encouraged for Internet access on entry to the school. Students should not be prevented from accessing the internet unless the parents have specifically denied permission or the child is subject to a sanction as part of the school behaviour policy.

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff will read and sign the relevant policies contained within the Staff Handbook.
- Parents will be asked to read the School Acceptable Use Policy for student access and discuss it with their child.
- All visitors to the school site who require access to the school's network or internet access will be asked to read and sign a Visitor Acceptable Use Policy. It is the responsibility of the member of staff who has invited the visitor to the School to ensure that this happens prior to them using ICT equipment.

5.2.12 Risk Assessment for On-line safety

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the fact that it is not possible to completely remove the risk that students might access unsuitable materials via the school system. It is wise to include a disclaimer, an example of which is given below.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish whether the E–Safety policy is adequate and that the implementation of the E–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Senior Leadership Team and ICT Network Manager.
- Methods to identify, assess and minimise risks will be reviewed regularly.

5.2.13 On-line safety Incidents and Complaints

5.2.13.1 Reporting of Incidents or Concerns

On-line safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Staff are the first line of defence; their observation of behaviour is essential in recognising concerns about students and in developing trust so that issues are reported.
Staff should also help develop a safe culture by observing each other's behaviour on-line and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Safeguarding Person.
Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve the Police should be made as soon as possible, after contacting the Safeguarding Children in Education team, if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting on-line safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- On-line safety concerns need to be reported in the same way as a safeguarding concern
- The ICT Network Manager or Designated Safeguarding Person will record all reported incidents and actions taken in the School on-line safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Safeguarding Person will be informed of any on-line safety incidents involving safeguarding concerns, which will then be escalated appropriately.
- The school will manage on-line safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Police.
- If the school is unsure how to proceed with any incidents or concerns, then the incident may be escalated to the Local Authority On-line Safety Officer.
- If an incident or concern needs to be passed beyond the school, then the it will be escalated to the ICT Network Manager or Designated Safeguarding Person to communicate to other local schools.

5.2.13.2 Handling of On-line Safety Related Complaints

Parents, teachers and students should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. On-line safety incidents may have an impact on students, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.
A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy. Potential safeguarding or illegal issues must be referred to the school Designated Safeguarding Person or On-line Safety Coordinator. Advice on dealing with illegal use can, when deemed necessary, be discussed with the Police and CEOP.

- Complaints about Internet misuse will be dealt with under the School's complaints policy procedure.

- Any complaint about staff misuse will be referred to the Headteacher.
- All On-line safety complaints and incidents will be recorded by the school, including any actions taken.
- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and safeguarding procedures.
- All members of the school community will be reminded about safe and appropriate behaviour on-line and the importance of not posting any content, comments, images or videos on-line which cause harm, distress or offence to any other members of the school community.

5.2.14 Communication of On-line Safety Policy

5.2.14.1 Students

- All users will be informed that network and Internet use will be monitored; this is covered in ICT lessons in Year 7 Unit 7.0.
- An on-line safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- Student instruction regarding responsible and safe use will precede Internet access.
- An on-line safety module will be included in the PSHCE and ICT programmes covering both safe school and home use.
- On-line safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to on-line safety education will be given where students are considered to be vulnerable.

5.2.14.2 Staff, governors and volunteers

It is important that all staff feel confident to use new technologies in teaching and the School On-line Safety Policy will only be effective if all staff subscribe to its values and methods.
Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.
If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.
Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. The School must be clear about the safe and appropriate uses of its school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.
ICT use is widespread and all staff including, administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school On-line Safety Policy.

- The On-line Safety Policy will be formally provided to and discussed with all members of staff.

- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All members of staff will be made aware that their on-line conduct out of school could have an impact on their role and reputation within school, in line with current Teaching Standards. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

5.2.14.3 Parents and Carers

Internet use in students' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, students may have unrestricted and unsupervised access to the Internet in the home. The school helps parents plan appropriate use of the Internet at home and provides information about the risks.

- Parents' attention will be drawn to the school On-line Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to on-line safety at home and at school with parents will be encouraged.
- Parents will be requested to sign an on-line safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.
- Information and guidance for parents on on-line safety will be made available to parents in a variety of formats.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents on the school website.

Schools On-line Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for the on-line safety policy. Staff that could contribute to the audit include: Designated Safeguarding Person, SENDCO, On-line Safety Coordinator, Network Manager and Headteacher.

Has the school an on-line safety Policy that complies with Helsby High School guidance?	Y
Date of latest update: June 2018	
Date of future review: June 2020	
The school on-line safety policy was agreed by Governors on: July 2018	
The policy is available for staff to access at: RMStaff, Staff Handbook, Section H	
The policy is available for parents/carers to access at: Website in On-line safety Section	
The responsible member of the Senior Leadership Team is: Mrs Sam Warburton, Deputy Head	
The Governor responsible for on-line safety is: Mr T O'Neil	
The Designated Safeguarding Person is: Mrs Sam Warburton and Ms CAV Simmonds	
The On-line Safety Coordinator is: Mr S Ford, Strategic ICT Network Manager	
Were all stakeholders (e.g. students, staff and parents/carers) consulted with when updating the school On-line Safety Policy? PARENTAL FORUM/Digital Guardians	Y
Has up-to-date on-line safety training been provided for all members of staff? (not just teaching staff) (CEOP)	Y
Do all members of staff sign an Acceptable Use Policy on appointment?	Y
Are all staff made aware of the school's expectation around safe and professional on-line behaviour?	Y
Is there a clear procedure for staff, students and parents/carers to follow when responding to or reporting an on-line safety incident of concern?	Y
Have on-line safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y
Is on-line safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y
Are on-line safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Y
Do parents/carers or students sign an Acceptable Use Policy?	Y
Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y
Has an ICT security audit been initiated by SLT?	N
Is personal data collected, stored and used according to the principles of the GDPR 2018?	Y
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	Y
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y
Does the school log and record all on-line safety incidents, including any action taken?	N
Are the Governing Body and SLT monitoring and evaluating the school on-line safety policy and ethos on a regular basis?	Y

On-line Safety Contacts and References

CEOP (Child Exploitation and On-line Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Police in the usual way.

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix 1

OFSTED CONTEXT AND REQUIREMENTS
Excerpt from document "Inspecting On-line Safety OFSTED, Inspectors' Briefing"
Reference no: 120196

Recommendations for schools

The report recommended that schools:

☐☐audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies

☐☐work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school

☐☐use students' and families' views more often to develop on-line safety strategies

☐☐manage the transition from locked down systems to more managed systems to help students understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school

☐☐provide an age-related, comprehensive curriculum for on-line safety that enables students to become safe and responsible users of new technologies

☐☐work with their partners and other providers to ensure that students who receive part of their education away from school are e-safe

☐☐systematically review and develop their on-line safety procedures, including training, to ensure that they have a positive impact on students' knowledge and understanding.

Common risks students are likely to encounter

Please note that this is not an exhaustive list.

Content
☐☐exposure to inappropriate content, including on-line 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 on-line 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 on-line reputation

☐☐health and well-being (amount of time spent on-line (internet or gaming))

☐☐sexting (sending and receiving of personally intimate images)

☐☐copyright (little care or consideration for intellectual property and ownership (for example music and film))

Ofsted Key Features of Good and Outstanding practice

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of on-line safety issues. High quality leadership and management make on-line safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the On-line Safety Mark). A high priority given to training in on-line safety, extending expertise widely and building internal capacity. The contribution of students, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based on-line reporting processes that are clearly understood by the whole school, allowing the students to report issues to nominated staff, for example SHARP. Report Abuse buttons, for example CEOP.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT.
Policies	Rigorous on-line safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The on-line safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The on-line safety policy should incorporate an Acceptable Usage Policy that is signed by students and/or parents as well as all staff and respected by all.
Education	A progressive curriculum that is flexible, relevant and engages students interest; that is used to promote on-line safety through teaching students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others safety. Positive sanctions are used to reward positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider or RBC together with age related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting on-line safety. Using data effectively to assess the impact of on-line safety practice and how this informs strategy.

Indicators of inadequate practice

Personal data is often unsecured and/or leaves school site without encryption.

Security of passwords is ineffective, for example passwords are shared or common with all but the youngest children.

Policies are generic and not updated.

There is no progressive, planned on-line safety education across the curriculum, for example there is only an assembly held annually.

There is no internet filtering or monitoring.

There is no evidence of staff training.

Children are not aware of how to report a problem.

Sample OFSTED questions for students

1. If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?

2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?

3. Can you tell me one of the rules your school have for using the internet?

4. Do you understand what the risks of posting inappropriate content on the internet are (secondary students only)?

Sample OFSTED questions for staff

1. Have you had any training that shows the risks to your and students on-line safety?

2. Are there policies in place that clearly demonstrate good and safe internet practice for staff and students?

3. Are there sanctions in place to enforce the above policies?

4. Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and students?

5. Are their clear reporting mechanisms with a set of actions in place for staff or students who feel they are being bullied on-line?

6. Does school have any plans for an event on Safer Internet Day (note: this is an annual event now in its fifth year at least so any school who are engaged would know about it)?

Sample OFSTED questions for school leadership

Question	What OFSTED ar**e** looking for
1. How do you ensure that all staff receive appropriate on-line safety training that is relevant and regularly up to date?	• at least annual training (in-service or on-line) for all staff • training content changes each session to reflect advances in technology • recognised group or committee or individual with on-line safety responsibility • on-line safety certified professional(s) (CEOP, EPICT etc.)
2. What mechanisms does the school have in place to support students and staff facing on-line safety issues?	• robust reporting channels • on-line reporting mechanism (for example SHARP)
3. How does the school educate and support parents and whole school community with on-line safety?	• parent's on-line safety sessions • raising awareness through school website or newsletters • workshops for parents • children teaching parents (for example at sessions or in homework)
4. Does the school have on-line safety policies and acceptable use policies in place? How does the school know that they are clear and understood and respected by all?	• on-line safety policy is regularly reviewed • evidence that these are freely available (poster, handbooks, etc.) • children can recall rules • Children integral to policy production
5. Describe how your school educates children and young people to build knowledge, skills and capability when it comes to on-line safety? How do you assess its effectiveness?	• School assemblies • Programmes delivered across all age groups • Peer mentoring

Appendix 2

Staff Code of Conduct for Social Networking

Aims

- To set out the key principles and code of conduct expected of all members of staff, governors and volunteers at Helsby High School in relation to social networking.
- To further safeguard and protect children and staff.

The following are not considered acceptable:

- Use of the school's name, logo, or any other published material without prior written permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which link the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information or the disclosure of information or images which could compromise the security of the school.
- The posting of any images of employees, students, governors or other persons directly connected with the school while engaged in school activities without prior permission.
- In additional all members of staff, governors and volunteers must ensure that they:
    - Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school or anyone connected with the school.
    - Use social networking sites responsibly and ensure that their personal or professional reputation, or the school's reputation, is not compromised by inappropriate postings.
    - Are aware of the potential of on-line identity fraud and are cautious when giving personal information about themselves which may compromise their personal safety and security.
    - Do not communicate with any student studying at Helsby High School through a social networking site.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is contrary to the school's ethos and principles.
- The Governing Body will take appropriate action to protect the school's reputation and the reputation of all staff, parents, governors, children and anyone else directly linked to the school.

6.0 Monitoring and Reviewing the Policy

This policy shall be reviewed on a periodic basis and reissued. Period for review shall not exceed 12 months.

Student Acceptable Use Policy

New technologies have become essential to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet, other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. Young people should have a right to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and social use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, e-mail and other digital communications.
- Images must not be taken on personal devices unless I have permission of a member of staff to do so.
- I will not share any of my school passwords, nor will I try to use any other person's username and password.
- I will maintain my data and personal security: I will not give out my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- I must always log off when I leave a computer unattended on-line.
- I will immediately report anything unpleasant or anything that makes me feel uncomfortable when I see it on-line to a member of staff or by using the CEOP link.

I understand that everyone has equal rights to use technology as a resource and:

- That the school ICT systems are intended for educational use. I will not use the systems for any other use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or share images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to e-mails, unless I know and trust the person / organisation who sent the e-mail.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I am aware that some websites and social networks have age restrictions and I will respect this. I will NOT use any chat and social networking sites within school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, temporary exclusions, contact with parents and in the event of illegal activities involvement of the police.

Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile devices etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school e-mail, VLE, website etc.

Name of Student		
Tutor Group		
Signed		

General Data Protection Regulation
Acceptable Use Policy 2018

To achieve success by valuing others

Introduction

Helsby High School commits to protecting the privacy and security of the personal information it holds for staff, governors and volunteers. Please note our Privacy Statements.

To complement the data protection duties of the school there are duties shared by all staff, governors and volunteers because, as a professional organisation with responsibility for children's safeguarding, it is essential that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This agreement covers all digital and physical data systems, e.g. the internet, intranet, network resources, learning platform, software, communications tools (online and offline), equipment (access devices) and paper records, whether printed or handwritten and however stored.

1. I understand that data held by the school may only be processed (acquired, processed, stored, deleted or transmitted) on the legal bases that the school has registered with the Information Commissioner's Office.
2. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted. Any images or videos of students will always take into account parental consent. I will ensure that data no longer needed will be effectively deleted or shredded.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation. Such misuse is also covered by the GDPR and any such misuse must be reported to the ICO, and to the data subjects (people) affected, within 72 hours.
4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my device as appropriate.
5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password. I will adopt school procedures for the safe storage of my passwords and for acquiring new ones.
6. I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School Network to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft. I will not share any files or folders on the School Network with any other user. I will be mindful that when working in a public space that others may be able to see my laptop, tablet or mobile phone screen and will use my discretion as to whether information should be hidden from site. I am aware that enabling Bluetooth connectivity on mobile devices can be a security threat and will switch this off when it is not needed for a specific connection.

7. When using my own personal devices either in school or out of school to conduct school related activities, I will follow the rules set out in this agreement, in the same way that I would if I was using school equipment. I will also follow additional rules set out by the school in the Remote Working Policy, and ensure that any such devices are protected by up to date anti-virus software and free from viruses.
8. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will not try (unless I have permission) to make large downloads or uploads that may take up internet capacity and prevent other users from being able to carry out their work.
10. I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer setting, unless this has been approved by school policy.
11. I will respect copyright and intellectual property rights.
12. I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will immediately report any damage or faults involving equipment or software, however they may have happened.
13. I have read and understood the school's Data Security Policy and e-Safety Policy which cover the security of data and safe and appropriate access to data.
14. I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, radicalistic or extremist material, adult pornography covered by the Obscene Publications Act) or other inappropriate materials that may cause harm or distress to others. I will not try to use any programmes of software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
15. I will report all incidents of concern regarding children's online safety to the Designated Child Safeguarding Lead Mrs S Warburton and/or the e-Safety Coordinator and Strategic ICT Manager, Mr S Ford and/or the lead for Prevent Mrs S Warburton as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable/extreme websites to the e-Safety Coordinator.
16. My communications with students, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. All formal letters will be distributed through Student Services. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
17. I will refrain from using any form of social media to discuss any aspect of school life except purely social events that involve colleagues. I will follow any guidance issued when contributing to the use of social media by the school as an official communication channel. I must not bring the school or the profession into disrepute using social media. I must not engage with students using social media unless I am using a school approved account which is monitored.
18. My use of ICT and information systems and my written communication will always be compatible with my professional role whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites or postal addresses. My use of ICT and other forms of communication will not interfere with my work duties and will be in accordance with the school AUP and the Law.
19. I will not create, transmit, display, write, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.
20. I will promote e-Safety (including privacy) with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create. Similarly, I will promote care for others in the students' writing and any other content that they create.
21. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
22. The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being

used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I _____ (please print name) acknowledge that I have received and read and understood a copy of the Helsby High School Acceptable Use Policy.

Staff / Volunteer Name	
Signed	
Date	