E-Safety

Written By	Mrs D Dalton
Creation Date	November 2017
Adopted by Governors	21 December 2017
Last Review Date	N/A
Next Review Date	January 2020

1 Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Driffield School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2 Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The lead SLT member and e-safety co-ordinator in our school is Mrs D Dalton. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as East Riding Safeguarding of Children Board, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy .

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues.
- New staff receive information on the school's acceptable use and e-safety policies as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (please contact the Head of School or Deputy Headteacher)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas.

Managing the school E-Safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety information will be available via the school website, the school VLE (the HUB) and the e-safety noticeboard within the school.

3 E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school has a framework for teaching internet skills in ICT lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done both informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are made aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. house tutor/e-safety co-ordinator/teacher.
- Pupils are taught to critical evaluate materials and learn good searching skills through via the ICT curriculum.

4 Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and digitally agree to abiding by an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy.
- Users are provided with an individual network, email and Learning Platform log-in username.
- Pupils are not allowed to deliberately access materials or files on the school network, of their peers, teachers or others, unless these have been made publicly available.
- If you think your password may have been compromised or someone else has become aware of your password you should change your password immediately and report this to the e-safety co-ordinator.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

All use of the Driffield School computer network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- School internet access is controlled using a Smoothwall for Education UTM (Unified Threat Management Web Filter/Firewall)
- Our school also employs some additional web filtering which is the responsibility of the network manager.
- Driffield School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the network manager who will forward information to the e-safety co-ordinator if appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines. If there are any issues related to viruses or anti-virus software, the network manager should be informed immediately.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission the network manager.

6 Managing Web 2.0 Technologies

Web 2.0, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Pupils

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are reminded that posting material which may be construed as offensive relating to the school, pupils or staff, on any internet site is considered by the school as cyberbullying and appropriate action will be taken.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet unless the permission of the Head Teacher has first been given.
- The school e-safety co-ordinator will regularly monitor a range of popular interactive internet sites to ensure that no inappropriate material has been posted.
- Pupils who wish to create a social networking site for students of the school are requested to seek the permission of the Head Teacher. Where permission is granted pupils will be given permission to use approved school images. A condition of permission being granted is that the school e-safety co-ordinator will be a member of the site and will monitor that site from time to time.
- Our pupils are asked to report any incidents of bullying to the school via the house tutors.

Staff

- Staff are advised to employ caution when posting any material on the internet relating to themselves and their activities. The golden rule is to ensure that there would be no embarrassment or other consequences if something posted were read by the Head Teacher or pupils of the school.
- Staff are advised that, once posted on the internet, personal material may be publicly available for many years. All staff, and especially new staff, are therefore advised to check that no material about themselves can be found on the internet that would not meet the **golden rule**.
- (Remember that sometimes your image may be 'tagged' by other friends and acquaintances). Advice on this matter can be sought from the e-safety co-ordinator who will liaise with the Head Teacher and other staff if required.
- Staff are advised to use social networking and other similar sites (eg YouTube/Flickr) only with caution and to use the security features to ensure maximum privacy settings. Under no circumstances are staff allowed to accept a student as a 'friend' on any personal social networking site unless that student is a close relative (ie son/daughter/brother/sister etc). When posting, even with maximum privacy settings, staff are advised to remember the golden rule. Staff should seek the advice of the e-safety co-ordinator if required.
- Staff are advised only to create blogs, wikis or other web 2.0 spaces for educational purposes using the School Learning Platform where appropriate. However, in some circumstances this may be inappropriate (eg ICT staff teaching about web 2.0 technologies) in which case staff should consult the e-safety co-ordinator in advance to discuss and agree the most appropriate hosting website to use.
- Any video/images taken that show the school site and/or students in school uniform are considered to be inappropriate for uploading to the internet (whether for educational purposes or not) unless the permission of the Head Teacher has first been given.

7 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible

internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched off when inside the school buildings unless the responsible member of staff has directed otherwise.
- This technology may be used, on occasion for educational purposes. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission of the subject(s) must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission of the subject(s) must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

8 Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level four or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. An additional staff email address is available via the network manager upon request if staff wish to have an exclusive email address for use by pupils.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette ('netiquette'). This is particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication, never arranging to meet anyone without specific permission and virus checking attachments.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail (do not delete the email as it will be needed as evidence). This should be reported to the appropriate house tutor who may decide to forward this for action to the e-safety co-ordinator.
- Staff must inform the e-safety co-ordinator if they receive an offensive e-mail.
- Pupils are introduced to email as part of the ICT Scheme of Work when each student will be given their own school email account.

9 Safe Use of Images

Taking of Images and Film

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips and other residential visits. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.
- Where possible general shots of classroom or group activities should be taken rather than close-up shots of individual pupils. Care should be taken to ensure that students are in suitable dress (particularly relevant for PE activities). Staff should also be mindful of including images of children from different ethnic backgrounds and with disabilities to promote the school as an inclusive community and to comply with the Disability Discrimination Act.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Vulnerable Children

Staff need to be mindful of students whose status may change during their period at the school. For example a child's security may become at stake and extra precautions may need to be taken during that time to avoid publishing any image or other information regarding that child. Likewise, for any child who is 'looked after', it is the responsibility of the assistant head; inclusion to ensure that consent on the corporate parent's behalf is discussed with the child's social worker.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use and store their child's work/photos in the following ways:

- on the school computer network
- on the school web site
- on the school's Learning Platform (the HUB)
- on the internet uploaded to websites previously approved by the headteacher or e-safety co-ordinator
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school

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

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.
Parents/ carers may withdraw permission, in writing, at any time.

Pupils' full names will not be published alongside their image (ie either image and first name or full name with no image). E-mail and postal addresses of pupils will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- The network manager has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only person with access to this is the site manager.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Video Conferencing

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

Parental right to take photographs and videos

Parents are permitted to take photographs and videos at school events for their own personal use only (unless this is expressly prohibited – for example at school plays where there are third party copyright regulations which prohibit recordings). Recording and/or photographing other than for private use would require the consent of other parents whose children may be captured on film. Without this consent, the Data Protection Act 1988 would be breached.

Official School Photographs

From time to time the school will invite an official photographer into school to take photographs of individual children and house/form groups. The school will ensure that appropriate CRB checks have been made with the company concerned.

10 Misuse and Infringements

Complaints and Reports

Complaints and reports relating to e-safety should be made initially to the e-safety co-ordinator who will then liaise with other members of staff/students/parents as appropriate. The only exception to this is with

incidents of cyberbullying when the house tutor is generally the first point of contact. The house tutor, in this instance, will liaise with the e-safety co-ordinator. All incidents will be logged and appropriate action taken and recorded.

The e-safety co-ordinator can be contacted on 01377 253631 ext 263.

Sanctions
A variety of sanctions may be used according to the type and seriousness of the incident. These may include, but are not limited to:

- An internet ban for a fixed period
- A ban from the school network for a fixed period
- A ban from bringing mobile phones etc onto the school premises
- A verbal/written warning
- A lunchtime/after-school detention
- Withdrawal from lessons for a fixed period in internal isolation
- Exclusion for a fixed period
- Permanent exclusion

Inappropriate material

- All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the network manager who will forward information to the e-safety co-ordinator if appropriate.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct of the school computer network as part of the acceptable use policy which they must signed up to.

11 Equal Opportunities

Pupils with additional needs

- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules. However, staff are aware that some pupils may require additional teaching including (visual) reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
- Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.
- Some students may find it difficult to explain or describe events and may need to replay (distasteful) scenarios in order to aid their recall. Some students may not be aware of the consequences of their actions or that they may require or should ask for help at all. Sensitive and context-dependant handling of such issues by staff is required.

12 Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy by contacting the e-safety co-ordinator to discuss e-safety issues. Contact details are widely publicised.

- Parents/ carers are asked to read through the school acceptable use agreements that their child has been asked to sign up to.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to e-safety where appropriate in the form of;
    - Information evenings, displays and posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training

13 Writing and Review of the E-Safety Policy

Our e-Safety Policy has been written by the school, building on the Hertfordshire Grid for Learning exemplar policy (with acknowledgement to LGfL, SWGfL and Bristol City Council) and Becta guidance.

Review Procedure

- There will be an on-going opportunity for staff to discuss with the e-safety co-ordinator any issue of e-safety that concerns them.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Key

KS3 – Key stage 3 (years 7-9)
KS4 – Key stage 4 (years 10-11)
KS5 – Key stage 5 (years 12-13)
NC - National Curriculum
SLT - Senior Leadership Team
SEN - Special Educational Needs
Alps - Key Stage 5 data and target setting package
AS - Advanced Subsidiary (qualification)
HOH - Head of House
AFL -Assessment for Learning
DFE – Department for Education
JCQ – Joint Council for Qualifications
LA – Local authority
ERYC – East Riding of Yorkshire Council

ACCEPTABLE USE OF ICT (Key points for staff)

Equipment

- Should you require any software and/or hardware installed on the school network always get permission and/or seek advice from the ICT technical support team.
- Damaging or disabling resources is strictly forbidden. If a piece of equipment is not functioning as required, please contact the ICT technical support team.
- Always check files brought in on removable devices with antivirus software and only use them if they are found to be clean of viruses.
- School Laptops should, at regular intervals (at least once per month), be plugged into the network to install anti-virus updates.
- Do not let family members use the school ICT equipment (laptop, IPads etc) these are supplied for use by staff only.
- You have the ability to install your own software on your school devices. It is your responsibility to ensure that any software that you install is legal.
- IPads should not be removed from their protective cases.

Portable Storage Devices (USB Pen drives/hard Drives)

Staff must ensure that all devices taken off site will be secured in accordance with the Data Protection Registration. Sensitive or confidential data should not be stored on portable computing devices or portable storage media unless password protected or encrypted. Physical security measures shall, at a minimum, include:

- Portable computing devices and storage media must be stored in a secure environment.
- When in public places (even your office, if it is not locked) users must ensure portable devices and storage media remain in the close proximity and are never left unattended.
- Staff must avoid unauthorised viewing of sensitive or confidential data in public, home or common areas.
- Staff must not leave portable devices and storage media in an unattended vehicle.

Security and Privacy

- Ensure that you use a suitably complex password for access to the Internet and ICT systems. Please note the following:
    - Keep passwords secure from pupils, family members and other staff
    - Use a different password for accessing school systems to that used for personal (non-school) purposes
    - Do not allow passwords to be remembered automatically within the machine internet browser or any other remote access software
    - Lock the computer when leaving it using CTRL+ALT+DEETE
    - Do not disable the passcode on your school IPad
- Never use someone else's logon name or password
- Proceed with caution when asked to disclose any personal details. (address, telephone number, pictures etc.)
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- Respect the security of the network.
- School computers are shared resources and thus should not be used for personal use, as there is a risk that private/confidential information could fall into the wrong hands (Bank, Credit card details and other personal information)
- Internet access is filtered for the benefit of all users. Any anomaly of sites that are filtered or not, should be reported to the ICT support team
- **In order to safeguard you and others, the school reserves the right to monitor communications**, examine or delete any files that may be held on its computer systems.
- **You have personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information**

Internet

- Access of the Internet should be for school purposes.
- Limited personal use of the internet is permitted in your own time only (i.e. during lunch breaks, prior to the start of the working day, at the end of the working day and for teaching staff during break times and free periods). This use must be in line with the guidance in this policy.
- Only access suitable material; using the Internet to obtain, download, send, print, display, transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people both outside and inside the school. This includes abiding by copyright laws.

Email

- Be polite and appreciate that other users might have different views from your own.
- Only open attachments to emails if they come from someone you already know and trust.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, report such messages to a member of ICT support team
- **When communicating on behalf of school <u>only</u> use your school email address for all correspondence with staff, parents or other agencies.**
- Limited personal use of the email is permitted in your own time only (i.e. during lunch breaks, prior to the start of the working day, at the end of the working day and for teaching staff during break times and free periods). This use must be in line with the guidance in this policy.
- Email is recognised as a proper method of communication within school but must not be used as a way of avoiding traditional means of communication, for example email must not be used to impart information that should be exchanged face-to-face.
- It is easy to unintentionally write an email in a threatening manner. Employees must take care not to send aggressive emails which are often referred to as "flame" mails. A "flame" mail is generally a

response that is sent in the heat of the moment and conveys emotion or feeling which may not be appropriate. It is advisable that employees should allow the situation to “cool down” before responding.
- Computer screens must always be locked when a user leaves the immediate vicinity to prevent unauthorised usage of the logged-in email account.

Mobil**e phones and Devices**

- Do not contact parents or pupils on personally-owned devices.
- Do not use personally-owned mobile devices to take images or sound recording.

Social Media

- You should set and maintain a profile on social networking sites to maximum privacy and give access to known friends only.
- Do not use social media tools to communicate with current students under the age of 18.
- If you experience derogatory or slanderous comments relating to you, the school or colleagues, take screenshots for evidence and report to the school ICT support team. Do not respond to these communications directly.

VLE (the HUB)

The School VLE is deemed to be an extension of the school network and as such is governed by the Acceptable Use Policy. Staff must only access the school network remotely using their school laptop/ IPad.