E-Safety Policy
This policy refers to:
Ysgol Harri Tudur / Henry Tudor School

Head Teacher: Mrs Fiona Kite

Author: Ross Harries, IT Network Manager

Date Created: 1st March 2022

Date of Next Review: Governor Resources Committee Autumn 2022

Published on Website: Yes

Contents

1. Overview

1.1 Policy Aims

The school recognises that Information Technology (IT) and the Internet are excellent tools for learning, communication and collaboration and can bring many benefits to pupils, staff and parents. The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions and the school will endeavour to equip pupils with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave Ysgol Harri Tudur / Henry Tudor School. It is also an important part of the school's pastoral care programme to ensure that pupils are provided with the education and resilience needed to protect themselves and their peers from online dangers.

Technology is advancing rapidly and is now a large part of everyday life, education and business. However, it is important that all members of the school community are aware of the potential dangers of using the internet and understand the importance of using it appropriately.

The school has a 'duty of care' towards any staff, pupils or members of the wider school community, to educate them in e-safety and this policy governs all individuals who are given access to the School's IT systems. This could include staff, governors, volunteers and pupils.

The school understands that some adults and young people will use technologies to harm children and there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in school and providing members of the school community with a good understanding of appropriate IT use outside of school hours.

E-safety does not just cover the Internet and available resources, but all different types of devices and platforms, for example, Smartphone devices, wearable technology and other electronic communication technologies. These are accessible within the school for enhancing the curriculum, to challenge pupils, and to support creativity and independence.

Some of these technologies and processes are already detailed in separate School Policies and, where appropriate, annexed to this Policy.

1.2 Training

The school provides e-safety guidance to staff to better protect pupils and themselves from online risks and to deal appropriately with e-safety incidents as and when they occur. Ongoing staff development includes training in online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

1.3 Policy Availability and Communication

E-Safety is integrated into the curriculum in any circumstance where the internet or technology is being used, as well as being specifically addressed in the PSHE curriculum. On joining the school, all staff must read the Staff Code of Conduct and staff and pupils must agree to comply with the IT Acceptable Use Policy before accessing the school IT systems.

Only staff with a contract of employment and pupils who are on roll are granted access to the schools IT Systems.

1.4 Roles and responsibilities

E-safety is the responsibility of the whole school community. The Senior Leadership Team (SLT) has overall responsibility for this policy. They will work closely with the IT Network Manager, the Director of Health & Wellbeing and senior pastoral and academic staff in this regard.

The Governing Board undertakes a regular review of the school's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the school's curricular provision, ensuring relevance, breadth and progression.

1.5 Systems & security

The school takes the protection of school data and personal protection of the school community seriously. This requires protecting the school network, (as far as is practicably possible), against viruses, hackers and other external security threats. The IT Delivery Group[1] is responsible for reviewing and managing the security of the IT services and networks that the school operates, and the security of the school information systems and users is reviewed regularly by the IT Support team.

Anti-Virus and Malware protection software is updated regularly. Other safeguards that the school takes to secure computer systems include:

- Making sure that unapproved software is not downloaded or installed onto any school computers and that files held on the school network are regularly checked for viruses
- Ensuring that unique user logins and passwords are always used to access the school network
- Internet connections are appropriately firewalled and secured

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils and some is age specific. The school takes all reasonable precautions to ensure that users access only appropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer or device connected to the school network.

2. Guidance for pupils and staff

2.1 Email

Email is an essential part of school communication. It is used internally by staff and pupils, and externally in conducting the day-to-day business of the school.

The school has the right to monitor emails and attachments where there is suspicion of inappropriate use and access in school to external personal email accounts may be blocked. Further guidance on this area is contained within the Ysgol Harri Tudur / Henry Tudor School Code of Conduct for IT Administrators (see Annex 6).

2.1.1 Staff should be aware of the following when using email in School:

- Staff should only use their school email accounts for school-related matters, including contact with other professionals, pupils, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent externally from school email accounts should be professional and carefully written. Staff are always representing the school and should take this into account when entering into any email communications.
- Emails sent internally should be as equally professional and courteous as those sent externally. Staff should not write anything to colleagues which they would not be happy to deliver face to face.

[1]The ITDG comprises of Deputy Head (Curriculum), SBM, Network Manager, SLT Curriculum lead and senior IT teaching staff

- The school permits the incidental use of staff school email accounts to send personal emails if such use is kept to a minimum and takes place out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the school, nor should it include or refer to anything which may bring the school into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any member of staff has breached these requirements, disciplinary action may be taken.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their Head of Department or a senior member of staff.
- Staff must tell their Director of Faculty or member of SLT and the IT Network Manager if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. **They should not attempt to deal with this themselves.**
- The forwarding of chain messages is not permitted in School.
- Incoming email should be treated as suspicious, and attachments not opened unless the author is known.

The full protocol for staff use of the Internet and email is set out in the IT Acceptable Use Policy (Annex 2 of this document).

2.1.2 Pupils should be aware of the following when using email in School:

- All pupils are provided with a school email account and pupils may only use approved email accounts on the school system.
- Pupils are warned not to reveal personal details of themselves or others in email communication or arrange to meet anyone. Excessive social emailing can interfere with learning and in these cases, will be restricted.
- Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. **They should not attempt to deal with this themselves.**
- The forwarding of chain messages is not permitted in school.
- Incoming email should be treated as suspicious, and attachments not opened unless the author is known.

2.2 Social Media

Social media sites have many benefits, however both staff and pupils should be aware of how they present themselves and the school online. Pupils are taught through the IT curriculum and Health & Wellbeing about the risks and responsibility of using social media, including the dangers of uploading personal information and the difficulty of taking it down completely once uploaded (often referred to as a "digital footprint").

The IT Department restricts access to social networking sites via the school network for both pupils and staff. Access is granted only when the requirements of a subject being taught in the school require it.

Staff use of other communication platforms such as WhatsApp is permitted on the proviso that it is used in connection with school related matters.

Please refer to the school's social media Policy for further details, (Annex 3 of this document).

2.3 School website and external marketing

The school website is the primary medium for communicating to parents and the wider community. Any information published on the website is carefully considered in terms of safety for the school community.

A small team of staff, under the direction of the IT Delivery Group and SLT are responsible for publishing and maintaining the content of the school website.

2.4 Use of digital images

Photographs and pupils' work bring the school to life, showcase pupils' talents, and add interest to publications both online and in print that represent the school. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material. Please see the School's Taking Storing and Using Images of Children Policy for full guidance (Annex 4 of this document).

2.5 Evaluating Internet Content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum and pupils are taught to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news").

2.6 Copyright and plagiarism

Pupils are taught to acknowledge the source of information used and to respect copyright. The school take any intentional acts of plagiarism seriously; any alleged events will be onvestigated and, where appropriate, action taken.

2.7 Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. It is more fully defined within the School's Anti-Bullying Policy, which sets out specific strategies to prevent and tackle bullying and is available on the school website.

2.8 Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational and pedagogical benefits that they might have. The school keeps up-to-date with modern technologies and is prepared quickly to develop appropriate strategies for dealing with new technological developments.

2.9 Personal Data

Personal data is recorded, processed, transferred and made available according to the Data Projection Act 2018 and EU General Data Protection Regulation 2016. Please see the School Data Protection Policy and Relevant Privacy Notices for further guidance.

3. **Concerns and identifiable Risks**

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Safeguarding Policy and Child Protection Procedures (available on the school website).

Such risks may include, but are not limited to, inappropriate contacts and non-contact sexual abuse, online child sexual exploitation, contact with violent extremists or children accessing websites advocating extreme or dangerous behaviours.

If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to the IT Department or any member of the management team. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the IT Network Manager or a member of the Management/Leadership Team.

Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective. The responsibility for these reports and checks falls to the IT Network Manager and Designated Safeguarding Lead, however the responsibility may be delegated to others within those teams. Reports are produced monthly by the IT Department and given to the Designated Safeguarding Leads (DSLs) for Pupils and to the HR Department for staff. It is the responsibility of the DSLs and/or the Director of HR to action items in those reports and to request any sanctions if required.

4. Fair Wear and Tear and Damage.

School is funded and equipment with a significant number of IT items to support pupil education. It is accepted that such equipment will be subjected to wear and tear and need to be replaced and upgraded over time; this is part of planned and funded maintenance. Where equipment is deliberately damaged and blame can be attributed, appropriate action will be taken to recover the costs of such damage from pupils and their families.

Annex 1: Mobile Technology Policy

1. **Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology**

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

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

The school's expectation is that mobile devices will be used responsibly at all times and pupils are required to adhere to the following rules:

2. **School rules on pupils' use of mobile phones**

Pupils may bring a mobile phone or other portable electronic devices to school – Bluetooth speakers should not be brought to school. Mobile phones, headphones or other portable devices cannot be used in school except in the following circumstances:

- Improper use will result in the phone (or device) being confiscated.
- If a phone (or device) is confiscated, it will be taken to Pupil Support for safe keeping.
- It will be placed in an envelope and the personal details of the pupil written on the envelope. The phone may be collected at the end of the day at 15:15.
- Repeated misuse will result in the phone (or device) being confiscated and a call home to a parent to discuss the misuse. It may also result in a temporary or permanent ban on the device being allowed in school.

3. **School rules on staff use of mobile phones and other technology**

Staff are expected to model good conduct in the use of mobile technology and, where possible, set an example by following the rules that pupils are expected to follow in relation to mobile technology. There are necessary exceptions to this, of course, and some staff must be contactable on their mobile phone at all times.

In safeguarding themselves and others, staff must adhere to the following guidelines:

- Staff must not share their personal mobile telephone number with pupils or parents;
- Staff must not text or instant message a pupil or parent using their personal mobile phone (or mobile device);
- Staff are provided with school mobile phones when on trips in order to mitigate against any need to share personal numbers with pupils or parents.
- If staff need to contact parents using their personal mobile phone, staff are instructed to block their mobile telephone number so that it does not appear on a parent's phone (See Annex 7 for instructions on how to block the mobile number).

Annex 2: IT Acceptable Use Policy

1. **Introduction**

- Ysgol Harri Tudur / Henry Tudor School is committed to protecting its Governors, staff, parents, pupils, volunteers and associated third parties, (known as the school community), from illegal or damaging use of technology by individuals, either knowingly or unknowingly.
- As users of the School's IT services individuals have a right to use its computing services; that places responsibility on these users which are outlined below.
- Ignorance of this policy and the responsibilities it places on users is not an excuse in any situation where it is assessed there has been a breach of the policy and its requirements.
- Individuals who connect their own IT equipment to the school's BYOD network and the services available (including the use of 3G and 4G) are to comply with this policy document.
- All employed staff are required to acknowledge their adherence to and compliance with this policy document when they first log on to the network.

2. **Purpose**

The purpose of this policy is to:

- Outline the acceptable and unacceptable use of technology including "online services", owned or operated by the school or by a School approved third- party, and acceptable or unacceptable general behaviour in IT areas;
- Educate and encourage individuals to make good use of the business and educational opportunities presented by access to technology.
- Safeguard and promote the welfare of the school community, in particular by anticipating and preventing the risks arising from:
- Exposure to harmful or inappropriate material (such as (but not limited to) pornographic, racist, extremist or offensive materials);
- The sharing of personal data, including images;
- Inappropriate online contact or conduct; and
- Cyberbullying and other forms of abuse;
- Help individuals take responsibility for their own safe use of technology (e.g. limiting the risks that individuals are exposed to when using technology);
- Ensure that the school community use technology safely and securely and are aware of both external and peer to peer risks when using technology.

These rules are in place to protect the school community. Inappropriate use exposes the school and its associated third-party partners to risks including virus attacks, compromise of network systems and services, and legal issues.

3. **Scope**

- This policy applies to all the school community at Ysgol Harri Tudur / Henry Tudor School as outlined in section 1 of this Annex.
- The school will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including, (but not limited to):
    - The internet;
    - Email;
    - Mobile phones and smartphones;
    - Desktops, laptops, netbooks, tablets;
    - Personal music players;
    - Devices with the capability for recording and / or storing still or moving images

- Social networking, micro blogging and other interactive web sites;
- Instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;
- Webcams, video hosting sites (such as YouTube);
- Gaming sites;
- Virtual Learning Environments;
- Interactive Boards;
- Other photographic or electronic equipment e.g. GoPro devices and other wearable technology.

- This policy also applies to the use of technology on and off school premises if the use involves any member of the school community or where the culture or reputation of the school or a member of staff are put at risk.

4. **Responsibilities**

- This policy is the responsibility of the IT Delivery Group with input from the Senior Leadership Team as and when required.
- The Business Manager & IT Network Manager are responsible for ensuring that issues around data protection and copyright compliance are monitored.
- All Leadership and Management Team members are responsible for the implementation and monitoring of the policy.
- The responsibility for the supervision of the IT Acceptable Use Policy is delegated to IT Support. Any suspected breach of this policy should be reported to a member of IT Support staff. A responsible senior member will then take the appropriate action within the school's disciplinary framework; other members of the School IT Support staff will also take action when infringements are detected in the course of their normal duties. All incidents involving the safe use of technology will be logged.
- The Designated Safeguarding Lead will consider the record of incidents and logs of internet activity as part of the ongoing monitoring of safeguarding procedures.
- Consideration of the efficiency of the school's online safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

5. **Safe use of technology**

- Pupils may find the following resources helpful in keeping themselves safe online:
  - http://www.thinkuknow.co.uk
  - http://www.childnet.com
  - http://www.childline.org.uk/Pages/Home.aspx

6. **Procedures**

- Individuals are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If an individual is aware of misuse by others they should talk to a teacher or Senior Manager about it as soon as possible.
- Any misuse of technology by pupils will be dealt with appropriately. Any misuse by staff will be dealt with under the School's Disciplinary Procedure. Any misuse by other members of the School Community may be dealt with through legal procedures.
- Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti- Bullying Policy.
- In any cases giving rise to safeguarding concerns, the matter will be dealt with under the school's child protection procedures (see the School's Safeguarding Policy & Child Protection Procedures). If an individual is worried about something that he / she has seen

on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a member of staff as soon as possible.

- In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead (ALNCO) who will record the matter and follow the procedures set out in the School's Safeguarding Policy and Child Protection Procedures.

7. **Unacceptable Usage**

- Unacceptable use of School technology and network resources may be summarised as, but not restricted to:
    - Actions which cause physical damage to any IT hardware, including peripherals (e.g. mouse, cables, wiring, and printers);
    - Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;
    - Viewing, retrieving, downloading or sharing any offensive material which may include content that is abusive, racist, considered to be of an extreme or terrorist related nature (including violence or extreme violence), sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity;
    - Threatening, intimidating or harassing staff, pupils or others;
    - Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
    - Defamation;
    - Unsolicited advertising often referred to as "spamming";
    - Sending emails that purport to come from an individual other than the person actually sending the message using, for example, a forged address;
    - Not adhering to the acceptable data storage levels set by the IT Department.
    - Attempts to break into or damage computer systems or data held thereon;
    - Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, e.g. use of equipment which is inadequately protected against viruses and spyware;
    - Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
    - Using the school network for unauthenticated access;
    - Any other conduct which may discredit or harm the school, its staff, community or the IT Facilities;
    - Using the IT facilities for gambling;
    - Using the IT facilities for carrying out any illegal trading activity.

8. **Sanctions**

- Where a user breaches any of the school rules, practices or procedures set out in this policy or the appendices, the School may apply any sanction which is appropriate and proportionate to the breach in accordance with the schools disciplinary procedures. Sanctions might include increased monitoring procedures and withdrawal of the right to access the school's internet and email facilities. Any action taken will depend on the seriousness of the offence.
- Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material.

9. **Key Principles and Rules**

- **Authorisation - access and security**

- In order to use the School's IT Facilities pupils must first be properly registered to use such services. Registration to use school services implies and is conditional upon acceptance of this IT Acceptable Use Policy.
- The registration procedure grants authorisation to use the core IT Facilities of the School. Following registration, a username and password will be allocated to each user. Authorisation for other services may be requested by application to the Wellington School IT Helpdesk.
- Any attempt to access or use any user account or email address, for which the user is not authorised, is prohibited.
- Users may not use, or attempt to use, IT resources allocated to another person, except when explicitly authorised.
- Users must take all reasonable precautions to protect the school's resources (including the IT Facilities and the School's information and data), their username and passwords.

- **Purpose of Use**
  - IT facilities are provided primarily to facilitate a person's essential work as a pupil or member of staff. Use for other purposes, such as personal email or recreational use of the Internet, is only permitted during the permitted times specified by the school and is a privilege, which can be withdrawn at any time and without notice. Any such use must not interfere with the pupil's studies or any other person's use of computer systems and must not, in any way, bring the school into disrepute.
  - School email addresses and associated school email systems must be used for all official school business. All users must regularly read their school email and delete unwanted or unnecessary emails at regular intervals.
  - The school has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. Users must not try to bypass this filter.
  - Viruses can cause serious harm to the security of the school's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If a user thinks or suspects that an attachment, or other downloadable material, might contain a virus, they must speak to a member of IT Support staff before opening the attachment or downloading the material. Users must not disable or uninstall anti-virus software on the school's computers.
- **Privacy and Monitoring**
  - All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Users are personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person.
  - Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.
  - For the protection of all users, their use of email and of the internet when accessed via the school network will be monitored by the school. Users should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Users should not assume that files stored on servers or storage media are always private
  - Users must not interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, users must not make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

10. **Use of the internet**

- Users must take care to protect personal and confidential information about themselves and others when using the internet, even if information is obtained inadvertently
- Users must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature (including violence and extreme violence), sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Users must inform a member of the Safeguarding Team immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.
- Pupils must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.
- Users must not bring the school into disrepute through their use of the internet.
- The school does not undertake to provide continuous Internet access. Email and website addresses at the school may change from time to time.

11. **Copyright Compliance**

- All users must abide by laws relating to the use and protection of copyright.
- Users must not download, copy or otherwise re-produce material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose e.g. research then copyright permission must be obtained and documented before such material is used.
- The school treats plagiarism very seriously and will investigate any allegation.

12. **Use of email**

- Pupils must use their school email accounts for any email communication with staff and vice versa.
- Email should be treated in the same way as any other form of written communication. Users should not include or ask to receive anything in an email which is not appropriate to be published generally or which they believe the school would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone they did not intend.
- Users must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature (including violence and extreme violence), sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If pupils are unsure about the content of a message, they must speak to a member of staff. If they come across such material, they must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.
- Trivial messages and jokes should not be sent or forwarded through the school's email system. Not only could these cause distress to recipients (if considered to be inappropriate) but could also cause the school's network to suffer delays and / or damage.
- Users must not read anyone else's emails without their consent.

13. **Use of mobile electronic devices**

- "Mobile electronic devices" includes but is not limited to mobile 'phones, smartphones, tablets, laptops and MP3 players.
- The use of mobile electronic devices is permitted in specified circumstances provided that usage is in accordance with the School Rules.
- Pupils, when permitted to use their mobile electronic devices may use their devices on the Student Wi-Fi network only. Pupils are not permitted at any time to connect devices with a network cable in any part of the school or to any other school Wi-Fi network.
- Pupils must not communicate with a member of staff's personal (as opposed to School) mobile phone.
- On occasions where it is deemed necessary, such as an educational visit, relevant staff will be issued with a School mobile phone, which they must sign out from the Network Manager. Pupils may then be provided with the school mobile number in the event that they need to contact that member of staff during the visit. Any such contact should be brief and courteous.
- Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not they are in the care of the school at the time of such use. Appropriate disciplinary action will be taken where the school becomes aware of such use (see the School's Anti-Bullying Policy and Promoting Good Behaviour policies) and the school's safeguarding procedures will be followed in appropriate circumstances (see the School's Safeguarding Policy and Child Protection Procedures.
- Mobile electronic devices may be confiscated in appropriate circumstances. Pupils may also be prevented from bringing a mobile electronic device into the school temporarily or permanently.
- The school does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

14. **Photographs and images**

- Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Pupils may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- Pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so. Phones can and will be searched where there is reason to believe that School Rules have been broken
- The posting of images which in the reasonable opinion of the school is considered to be offensive or which brings the school into disrepute on any form of social media or websites such as Facebook, YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

15. **Sexting (Youth Produced Sexual Imagery)**

- Sexting is strictly prohibited and any instances of sexting will be dealt with in accordance with the School's Safeguarding Policy and Child Protection Procedures.

Appendix 1 - IT Services Acceptable Use Policy (AUP) Summary

All users must ensure that they do not:

Allow other people to use your account.

- Download or access illegal software onto a workstation.
- Download or copy any software packages from the school network onto portable media, etc.
- Upload your own personal software packages onto a school workstation.
- Access offensive or abusive material.
- Send or receive offensive, abusive or inappropriate emails.
- Access "inappropriate" websites - some Internet pages are illegal and may be subject to criminal proceedings.
- Interfere with another user's work.
- Photograph or record members of staff or pupils without their permission, using devices such as mobile phones, cameras or digital recorders.
- Use software designed to unblock sites.
- Use online gambling sites.
- Use peer-to-peer and related applications anywhere on school premises. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus and KaZaA.
- Abuse equipment.
- Make offensive or inappropriate comments including bringing the school's name and reputation into disrepute on any forum/platform, such as social media sites (whether using a school device or not) where a connection between the user and Wellington School can reasonably be made.

When in teaching and learning areas such as the Library, IT Suites or classrooms;

- Keep noise to a minimum to avoid disrupting others.
- Copyright regulations apply to electronic sources - please check before you print out from online services.
- No unauthorised use of chat rooms.
- Logout or lock your computer when leaving a computer, even for a short time.
- Be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc.) has been electrically tested, before using it on School premises.
  Anyone found abusing the school policy on the use of computers may have their network rights removed, and may be subject to further disciplinary action.
- School computers are provided primarily for School work. However, you may use the equipment for personal use providing:
  - You do not breach the IT Acceptable Use Policy.
  - You are not doing so for gambling purposes.

If you use the school equipment for personal use, the user should note that;

- Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.
- If you are using communal IT facilities (such as the Library), you may be asked to log-off where the demand for the equipment is high.
- The IT Acceptable Use Policy applies to both wired and wireless access and use of network on your own equipment or on School equipment.
- Any user is not permitted to connect their device directly via cable to any network socket within the organisation or to any other Wi-Fi network that the school transmits.
- The school reserves the right to remove access to IT services at any time. Pupils must abide by all of this policy when their device is connected to the school network.

Annex 3 – Social Media Policy

Introduction

- The Internet provides a range of social media tools that allow users to interact with one another, from rediscovering friends on social networking sites such as Facebook to keeping up with other people's lives on Twitter and maintaining pages on Internet encyclopaedias such as Wikipedia.

  While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Ysgol Harri Tudur / Henry Tudor School Governors, staff, parents, pupils, volunteers and associated third parties, (known as the School Community), are expected to follow when using social media.

- It is crucial that the school community and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that all use social media responsibly so that confidentiality of the school community and the reputation of the school is safeguarded.

- Members of the School community must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

- This policy applies to all of the Ysgol Harri Tudur / Henry Tudor School Community, (as detailed above).

- This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the School

- This policy applies to personal web space such as social networking sites (for example Facebook, Instagram), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as Flickr and YouTube. The Internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Framework

- All members of the School Community are expected to act with integrity to ensure that they protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including, but not limited to:

  - The Human Rights Act 1998;
  - Common law duty of confidentiality;
  - The Data Protection Act 2018 and GDPR. Confidential information includes, but is not limited to:
    - Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 2018 and GDPR
    - Information divulged in the expectation of confidentiality
    - School business or corporate records containing organisationally or publicly sensitive information
    - Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and

- Politically sensitive information.

- The school community should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

    - Libel Act 1843;
    - Defamation Acts 1952, 1996 and 2013;
    - Protection from Harassment Act 1997;
    - Criminal Justice and Public Order Act 1994;
    - Malicious Communications Act 1988;
    - Communications Act 2003;
    - Copyright, Designs and Patents Act 1988.

- Ysgol Harri Tudur / Henry Tudor School could be held responsible for acts of members of the School Community. For example, staff members who harass co- workers online, or who engage in cyberbullying, discrimination, or who defame a third party while at work may render the school liable to the injured party.

Related Policies

- This policy should be read in conjunction with the following School policies and DfE guidance:

    - Safeguarding Policy and Child Protection Procedures
    - Staff Code of Conduct
    - IT Acceptable Use Policy
    - E-Safety Policy
    - Keeping Children Safe in Education (September 2021)
    - Working Together to Safeguard Children (July 2018)
    - Prevent Duty Guidance: for England and Wales

Principles - be responsible and respectful

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between school life and your personal interests.
- You must not engage in activities involving social media which might bring the school into disrepute.
- You must not represent your personal views as those of the school on any social medium.
- You must not discuss personal information about any other members of the school community or other professionals you interact with during the course of your school life on social media.
- You must not use social media and the Internet in any way to attack, insult, abuse or defame any member of the school community or other professionals, other organisations, or other Schools.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of the school.

Personal use of social media

Staff

- With the exception of professional online networking or employment sites, (e.g. LinkedIn, Reed), staff are strongly advised not to identify themselves as an employee of the School on

any personal social media pages. If a staff member does identify themselves then it is particularly important that they present a professional image at all times. Bear in mind that it is not always possible to control what appears on a Facebook page, for example, since Facebook can allow friends to post comments and photographs without prior approval.

- Staff members must not have contact through any personal social medium with any pupil or parent of a pupil, whether from the school or any other school, unless the pupils or their parents are family members.
- Any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.
- Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- On leaving the school's service, staff members must not contact the schools' pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.
- Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, other parties and School or Association corporate information must not be discussed on their personal webspace.
- Photographs, videos or any other types of images of pupils and their families or images depicting staff members wearing school uniforms or clothing with school logos or images identifying sensitive school buildings must not be published on any personal webspace. Staff should not post images or videos from school events on any public social media site. Images or videos taken at school events, when such permission has been granted by the school, are for the sole and private use of that individual and their use must be in accordance with the Data Protection Act 2018 and General Data Protection Regulations.
- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

  Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the School's IP address and the intervention will, therefore, appear as if it comes from the school itself.

- The school logos or brands must not be used or published on personal webspace.
- Access to social media sites for personal reasons is not permitted. However, staff members are expected to use their contracted hours of work to their professional duties and, in practice, personal use of the Internet should not be on the school's time.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Pupils

- Pupils are advised not to identify themselves as members of Ysgol Harri Tudur / Henry Tudor School in their personal web-space while as a pupil at the school. This is to prevent information being linked with the school and to safeguard the privacy of pupils. If a pupil decides to identify themselves, they should be mindful of the content that they post.

- Pupils should not have contact through any personal social medium with any member of staff, whether from Ysgol Harri Tudur / Henry Tudor School or any other school, other than those mediums approved by Ysgol Harri Tudur / Henry Tudor School, unless those staff are family members. If pupils and members of the wider school community wish to communicate with staff, they should only do so through official school sites created for this purpose.

Information that pupils and members of the wider community have access to as part of their involvement with the school, including personal information, should not be discussed on their personal web space. Photographs, videos or any other types of images of pupils and their families or images depicting staff members, clothing with school logos or images identifying school premises should not be published on personal or public web space without prior permission from the school.

- School email addresses are not be used for setting up personal social media accounts or to communicate through such media.
- Pupils should not edit open access online encyclopaedias such as Wikipedia in a personal capacity using a school computer system or Wi-Fi network. This is because the source of the correction will be recorded as the School's IP address and the intervention will, therefore, appear as if it comes from the school itself.
- All pupils are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
- All pupils should keep their passwords confidential, change them often and be careful about what is posted online. Pupils and the wider school community should not post images or videos from school events on any public social media site.
- Images or videos taken at school events, when such permission has been granted by the school, are for the sole and private use of that individual and their use must be in accordance with the Data Protection Act 2018 and General Data Protection Regulations.
- The school accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g. LinkedIn. The school expects due care and attention to be aken to maintain an up-to-date profile and a high level of presentation on such sites where Ysgol Harri Tudur / Henry Tudor School is referenced.

Using social media on behalf of the school

- Ysgol Harri Tudur / Henry Tudor School does not permit the use of social media platforms by staff and pupils.
- Staff must not set up a social media account for staff and pupil use. It is not permissible for staff to set up an account with parents, e.g. a Facebook account to share pictures during a school trip.

Inappropriate use of social networking sites by parents

The school considers the following examples to be inappropriate uses of social networking sites:

- Making allegations about pupils at the school/cyber bullying;
- Making complaints about the school/staff at the school;
- Posting negative/offensive comments about specific pupils/staff at the school;
- Posting discriminatory comments;
- Posting comments which threaten or incite violence.

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step, the school will usually discuss

the matter with the parent to try and resolve the matter and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school may consider taking one or more of the following actions:

- Set out the school's concerns in writing and request that the material in question is removed.
- Take legal advice and/or legal action if the circumstances warrant this;
- Contact the Police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed; or in cases where the posting has a racial or homophobic element, is considered to be grossly obscene or is threatening violence.

Monitoring of internet use

- Ysgol Harri Tudur / Henry Tudor School monitors usage of its Internet and email services without prior notification or authorisation from users.
- Users of school email and Internet services should have no expectation of privacy in anything they create, store, send or receive using the School's IT system.
- The school recognises that the use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology can provide the platform that facilitates harm. The school's approach to online safety endeavours to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:
    - content: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
    - contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
    - conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example

The school addresses these issues in the following ways:

- Appropriate filters and monitoring systems are in place to keep children safe online. The school uses a layered approach to monitor online behaviour. The technologies in use at the school including, but not limited to Smoothwall UTM, Panda AV, Watchguard, all of which monitor and filter all online activity on the school network;

    - monthly reports are sent to the Designated Safeguarding Lead (DSL) showing where a user has attempted to access a restricted website or concerning search criteria;
    - the systems aim to reduce the risk of children being exposed to illegal, inappropriate and harmful materials online; reduce the risk of children being subjected to harmful online interaction with others; and help manage online behaviour that can increase a child's likelihood of, or causes, harm;
    - children are regularly taught about safeguarding online, through Health & Wellbeing and assemblies;
    - staff are equipped with the knowledge to safeguard children online by attending online safety training;
    - due consideration is given to what online content is made available to pupils.

3G, 4G and 5G technology:

The school understands that many children have unlimited and unrestricted access to the internet through 3G, 4G and 5G via their personal mobile devices. The school addresses this issue in the following ways:

- the use of mobile devices by pupils up to year 11 is not allowed in school during the school day, with the exception of where a mobile device is being used in class under the instruction of a teacher for educational purposes or for a medical need.

Members of the sixth form are permitted to use their mobile phones in the common room or for the exceptions stated above.

- Through the availability of good Wi-Fi in the buildings pupils are encouraged to use the school's monitored and filtered, fast and free internet service rather than 3G, 4G or 5G.
- We recommend to parents that their child's mobile contract has "parental controls" enabled to help better ensure that their child cannot access harmful material while using the phone or other 3G, 4G or 5G device.
- We recommend that pupils are not given 3G, 4G or 5G Internet enabled dongles allowing them to browse the internet unrestricted ensuring that the School Internet is used to allow us to better safeguard your child.

The School's Safeguarding Policy and Child Protection Procedure also sets out the school's approach to online safety.

As part of the school's duties in tackling extremism and radicalisation, the schools' web filters are used to stop this content as recommended by Government guidelines. Attempted visits to these sites are monitored by the system and a notification message is sent to the Designated Safeguarding Leads (for pupils) and the HR Department (for Staff) should an access attempt be detected.

- **Breaches of this policy – Staff**

    - Any breach of this policy may lead to disciplinary action being taken against the staff member(s) involved in line with the School Disciplinary Procedures.

    - A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the School or any illegal acts or acts that render the School liable to third parties may result in disciplinary action or dismissal.

    - Contracted providers of the school must inform the relevant School officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors' internal disciplinary procedures.

Annex 4: Taking, Storing and Using Images of Children Policy

Aims

- This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Ysgol Harri Tudur / Henry Tudor School. It also covers the school's approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, and the media.

- It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of pupil images, including e.g. signage about the use of CCTV; and more general information about use of pupils' personal data, (e.g. the School's Privacy Notices). Images of pupils in a safeguarding context are also dealt with under the School's Safeguarding Policy and Child Protection Procedures.

- Certain uses of images are necessary for the ordinary running of the school; other uses are in the legitimate interests of the school and its community and unlikely to cause any negative impact on children. The school is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

- Parents who accept a place for their child at the school are invited to agree to the school using images of them as set out in this policy, by signing the Consent Form sent out with the School's Terms and Conditions (see Appendix 1). However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example, if they are included incidentally in CCTV or a photograph).

- With appropriate consent, school will use upil images to celebrate the achievements of pupils, sporting and academic, promote the work of the school, and for important administrative purposes such as identification and security.

- Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the school in writing. The school will always respect the wishes of parents/carers (and pupils) wherever reasonably possible, and in accordance with this policy.

Use of Pupil Images in School Publications

- With appropriate consent school will use images of pupils to keep the school community updated on the activities of the school, and for marketing and promotional purposes, including:

    - on internal displays (including clips of moving images) on digital and conventional notice boards within the school premises;

    - in communications with the school community (parents, pupils, staff, Governors and alumni) including by email, and by post;

      on the school's website. Such images would not normally be accompanied by the pupil's full name; and

    - in the school's prospectus, and in online, press and other external advertisements for the school. Such external advertising would not normally include pupils' names and in

some circumstances the school will seek the parent or pupil's specific consent, depending on the nature of the image or the use.

The school will only use images of pupils in suitable dress and the images will be stored securely and centrally.

Use of Pupil Images for Identification and Security

- Pupils are regularly photographed for the purposes of internal identification. These photographs identify the pupil by name, year group, house and form/tutor group.

Use of Cameras and Filming Equipment (including mobile phones) by Parents

- Parents are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

    - When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others.

    - Flash photography can disturb others in the audience, or even cause distress for those with medical condition, and is not to be used at indoor events.

    - Parents are not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.

      Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
    - Copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school will always print a reminder in the programme of events where issues of copyright apply.

    - Parents may not film or take photographs in changing rooms, the swimming pool or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.

The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or online digital copies may be made available to parents view or purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

Use of Cameras and Filming Equipment (including mobile phones)

- Where photographs are taken by staff to give evidence of pupils' progress, or to record a trip or sporting event, photographs can only be taken on school equipment. Staff must not use their own camera, mobile phone or tablet. Photographs/video must then be downloaded onto school computers. Photographs or video cannot be used or passed on outside the school.

- Neither staff nor children may use their own mobile phones to take photographs or video within our school setting.

- When taking photographs in School, staff must:
    - Be clear about the purpose of the activity and what will happen to the photographs when the lesson/activity is concluded;
    - Ensure that photographs are taken for valid educational purposes and, if in doubt, consult with their line manager;

  Ensure that all images are available for scrutiny in order to screen for acceptability;

    - Be able to justify images of children in their possession;
    - Avoid making images in one-to-one situations;
    - Not have images of pupils stored on personal cameras, devices or home computers;
    - Not make images of pupils available on the internet, other than through the official School network/website with permission from parents and senior leaders.

Use of Cameras and Filming Equipment by Pupils

- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of staff.
- The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.
- Pupils are not to film or take photographs of other members of the school community (pupils and staff), other than where there is a justifiable, educational reason. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- Where there is an allegation about a pupil taking inappropriate images, a senior member of the pastoral team may request access to images stored on mobile electronic devices and/or cameras and ask the pupil to delete the images in question. Photographs of any member of the school community are not permitted to be displayed publicly around the school campus unless in accordance with this Policy.
- The misuse of images, cameras or filming equipment in a way that breaches this Policy, or any of the school's other policies including but not limited to the Safeguarding Policy, Anti-Bullying Policy, Data Protection Policy and E-Safety Policy, is always taken seriously, and may be the subject of disciplinary procedures.

Annex 5: Code of Conduct for IT Systems Administrators

Policy Statement

Background

- Providing secure, high-availability, functionally-rich critical services in the Ysgol Harri Tudur / Henry Tudor School IT environment is a challenging responsibility. The scope of legislation and general scrutiny which applies to data security and accountability has increased dramatically over the past few years to the point where the school has been advised to set out clear guidelines.

Scope

- This code of conduct applies to all members of the organisation who are given Systems Administrator or elevated access privileges on any managed service, server or group of workstations.
- An individual who is granted elevated rights to IT systems is entrusted with operating the system or service on behalf of the school and for the benefit of all. An individual entrusted with this responsibility must always administer systems with this in mind.

Purpose

- The purpose of this document is to provide clear guidelines for members of the organisation who are Systems Administrators or who have been given elevated rights (Administrator, admin, root, Domain Admins or equivalent) to IT systems, to ensure a common, accountable, secure, and professional approach. Each person who is to be granted elevated rights is expected to read and commit to this code of conduct before rights are assigned. This specific code of conduct should be read alongside the generic Staff code of conduct to which all staff must equally adhere.

Authorisation and Authority

- Systems Administrators require formal authorisation from the "owners" of any equipment they are responsible for. The law refers to "the person with a right to control the operation or the use of the system". In Ysgol Harri Tudur / Henry Tudor School the IT Network Manager has the delegated authority, to decide which members of IT Services need to be allowed Systems Administrator status on any individual system or service, or a range of services, and when it is appropriate to change the ownership and scope of responsibility.

- The Director of Faculty (DoF) is usually the person with authority for departmentally provided services.

- If any administrator is ever unsure about the authority they are working under, they should stop and seek advice immediately from their direct line manager or the IT Network Manager, as otherwise there is a risk that their actions may be in breach of policy.

Responsibility

- 'Having responsibility' for an IT system, server, or service, means that a Systems Administrator is accountable for its successful operation, and is empowered to use experience, specialist skills, and judgement to make systems work in the most effective way. It does not mean that a Systems Administrator can make unilateral decisions about systems, or assume they are the only person who is permitted to make, or capable of making decisions about the systems they administer. Communication is a critical element in administering all systems, and a competent

Systems Administrator will, where possible, always review significant plans or changes with their direct line managers.

Permitted Activities

- The duties of Systems Administrators can be divided into two areas. The first duty is to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. Here the Systems Administrator is acting to protect the operation of the systems for which they are responsible. For example, investigating a denial-of-service attack, a defaced web server or the investigation of crime.

- The second duty is to monitor compliance with policies which apply to the systems. For example, the IT Acceptable Use Policy prohibits certain uses of the network. In these cases, the Systems Administrator is acting in support of policy, rather than protecting the operation of the system.

- The Systems Administrator should be clear, before undertaking any action, whether it is required as part of their operational or policy role. The two types of activity are dealt with separately in the following sections.
  Operational Activities
- Where necessary to ensure the proper operation of networks or computer systems for which they are responsible, authorised Systems Administrators may:

    - Monitor and record traffic on those networks or display it in an appropriate form;

    - Examine any relevant files on those computers;

    - Rename any relevant files on those computers or change their access permissions (see Modification of Data below);

    - Create relevant new files on those computers.

    - Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, the Systems Administrator must not attempt to make the content readable without specific authorisation from senior management or the owner of the file.

    - The Systems Administrator must ensure that these activities do not result in the loss or destruction of information. For example, if a change is made to user file store, then the affected user(s) must be informed of the change and the reason for it preferably prior, but as soon as possible after the event otherwise.

Policy Activities

- Systems Administrators must not act to monitor or enforce policy unless they have been requested to or informed by the IT Network Manager or Leadership team, who will ensure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies to which it will apply. If this has not been done through a general notice to all users then before a file is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or all the parties involved in a network communication.

Disclosure of information

- Systems and Network Administrators are required to respect the confidentiality of files and correspondence.

- During the course of their activities, Systems Administrators are likely to become aware of information which is held by, or concerns other users. Any information obtained must be treated as confidential - it must neither be acted upon, nor disclosed to any other person (including within the team except with your direct line manager) unless this is required as part of a specific authorised investigation.

- The IT Network Manager or Leadership Team will decide which information may be passed to managers or others involved in the investigation on a case-by-case basis. Information that emerges during an investigation, but does not relate to the current investigation, must only be disclosed if it is thought to indicate an operational problem, a breach of policy or a breach of law. It is the IT Network Manager or Leadership Team who decide whether further investigation is necessary and to who the information gathered should be passed onto.

- Systems Administrators must be aware of the need to protect the privacy of personal data and sensitive personal data, (within the meaning of the Data Protection Act 1998) that is stored on their systems. Such data may become known to authorised Systems Administrators during their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant Data Controller.

Modification of Data

- For both operational and policy reasons, it may be necessary for Systems Administrators to make changes to user files on computers for which they are responsible. Wherever possible this should be done in such a way that the information in the files is preserved:

    - rename or move files, if necessary to a secure off-line archive, rather than deleting them;

    - Instead of editing a file, move it to a different location and create a new file in its place;

    - remove information from public view by changing permissions (and if necessary, ownership).

Where possible the permission of the owner of the file should be obtained before any change is made, but there may be urgent situations where this is not possible. In every case the user must be informed as soon as possible what change has been made and the reason for it.

The Systems Administrator may not, without specific individual authorisation from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information or to seek personal gain.

Creation of Accounts

- Systems Administrators may have the capability to create user accounts on the systems they manage. They may only create accounts for individuals authorised by the organisation or the 'owner' of the system. Authorised users will normally be restricted to members of the school (i.e. staff, pupils, or others member(s) approved by Human Resources) and all such users must sign up to the School's IT policies to ensure regulations are understood and that staff / pupils can abide by computing and information security policies that are set out. Staff accounts are only to be authorised by the Human Resources team and not Heads of Department. Systems Administrator accounts for both Third-Party Suppliers and

elevated staff rights may only be setup and agreed by the IT Network Manager or IT Delivery Group and the Senior Leadership Team.

Enforcement

- Access to mailboxes and files are to be automatically logged and audited on a regular basis and any member of staff found in breach of any of the above policies or found to gain access to information for personal gain will be suspended with immediate effect without warning, pending investigation.
- The school recognises the above list is not exhaustive. As such the School retains the right to determine what is a 'breach of policy' on a case-by-case basis if individuals (governed by this policy) are investigated under disciplinary regulations.

Appendix 1

Reference and Acknowledgement

The following Acts are particularly relevant to the activities covered by this Code together with the guidance contained in the Information Commissioner's Codes of Practice.

www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct

1. The Data Protection Act (2018)
2. The General Data Protection Regulation 2016/679
3. The Human Rights Act (1998).

Annex 6 - CCTV Policy

- The purpose of this policy is to regulate the management and operation of the Closed-Circuit Television (CCTV) System at Ysgol Harri Tudur / Henry Tudor School. It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the school and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the System).

- The System is administered and managed by the school, who act as the Data Controller. This policy will be subject to review from time to time, and should be read with reference to the School's Data Protection Policy (available on the School Website).

- All fixed cameras are in plain sight on the school premises and the school does not routinely use CCTV for covert monitoring or monitoring of private property outside the school grounds.

- The school's purposes of using the CCTV system are set out below Data captured for the purposes below will not be used for any commercial purpose.

Objectives of the System

- To protect pupils, staff, and any other individual on and around our site with regard to their personal safety.

- To protect the school buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.

- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.

- To monitor the security and integrity of the school site and deliveries and arrivals.

- To monitor staff and contractors when carrying out work duties.

- To monitor and uphold discipline among pupils in line with the School's Promoting Good Behaviour and Exclusions Policies, which are available on the school website.

Positioning

- Locations have been selected, both inside and out, that require monitoring to address the stated objectives.

- Adequate signage has been placed in prominent positions to inform individuals that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.

- No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

  No images of public spaces will be captured except to a limited extent at site entrances.

Maintenance

- The CCTV System will be operational 24 hours a day, every day of the year.
- The System Manager(s), (defined below) will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.

- The System will be checked and (to the extent necessary) serviced no less than annually.

Supervision of the System

- Staff authorised by the school to conduct routine supervision of the System may include Facilities Staff, Senior Leadership Team and the IT team who are responsible for the maintenance and operation of the system.

- Images will be viewed by authorised staff and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

Storage of Data

- The day-to-day management of images will be the responsibility of the IT Department.

- Images will be stored for 3 to 4 weeks and automatically over-written unless the school considers it reasonably necessary to retain the images for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the Police or the Local Authority.

- Where such data is retained, it will be retained in accordance with our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and individuals recorded, will be noted in the system log book.

Access to Images

- Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access). Individuals who have been granted access will also receive relevant training on how to handle the data the system generates to ensure individuals' privacy.

- All individuals have the right to access personal data the school holds on them (please see the Data Protection Policy and Relevant Privacy Notices), including information held on the System, if it has been kept. The school will require specific details including at least the time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

- The System Manager must confirm the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

    - Where required to do so by the Head, the Police or some relevant statutory authority;

    - To make a report regarding suspected criminal behaviour;

    - To enable the Designated Safeguarding Lead or his/her appointed deputy(s) to examine behaviour which may give rise to any reasonable safeguarding concern;

    - To assist the school in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the school's management of a particular incident;

- To data subjects (or their legal representatives) pursuant to an access request under Data Protection and GDPR;

- To the School's insurance company where required in order to pursue a claim for damage done to insured property; or

- In any other circumstances required under law or regulation.

- Where images are disclosed under 6.3 above a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

- Where images are provided to third parties under 6.3 above, wherever practicable steps will be taken to obscure images of non-relevant individuals.

Other CCTV systems

- The school does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this is in line with the objectives of the school's own CCTV policy and/or its rules under the Promoting Good Behaviour and/or Exclusions Policy.

- Many pupils travel to School on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The school may request images from the coach companies in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the school's management of a particular incident.

Complaints and Queries

- Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the School Business Manager (SBM) in the first instance who has overall responsibility for the School's Data Protection. The IT Network Manager has delegated responsibility in the event the SBM is not available.

- For any other queries concerning the use of personal data by the school, please see the School's applicable Privacy Notice.

APPENDIX 1: CCTV FOOTAGE ACCESS REQUEST

(On Headed Paper)

Ysgol Harri Tudur / Henry Tudor School

EXTERNAL BODY CCTV FOOTAGE ACCESS REQUEST

The following information is required before the school can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the school typically deletes CCTV recordings after 3 to 4 weeks automatically.

Name:	
Address:	
Tel No:	
Email	

(Proof of ID may be required)

Description of footage:

Location of camera(s):

Date of footage sought	

Approximate time (give a range if necessary)

Signature:	
Print Name:	
Date:	

* NB if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.