# Ysgol Uwchradd Y Frenhines Elisabeth
# Queen Elizabeth High School

*Moving Forward Together*

# *E SAFETY POLICY*

**Date established by Governing Body: 6th December 2017**

**Responsible Person – Mrs S O'Kelly**

**Designated role – Assistant Head Teacher**

**Chair of Governors signature –** Helen Starkey

**Date – 06/12/2017**

# Policy Version Control

| Version | Date | Page | Section | Reason for review | Summary of amendment | Chair of Governor’s signature |
|---|---|---|---|---|---|---|
| 1 | 6/12/17 | | | New AHT appointed with responsibility for this policy. | | Helen Starkey<br>06/12/2017 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Contents:

## Schedule for Development/Monitoring/Review

Monitoring of the E-Safety Policy will take place at regular intervals.

The Governing Body will receive a regular report on safeguarding, including e-safety.

The E-Safety Policy will be reviewed in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

## Scope of the Policy

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

.
QEHS will deal with such incidents within this policy and associated behaviour and anti- bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place in and out of school.

## Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within QEHS.

### Governors

Governors are responsible for the approval of the e-safety Policy and for its review.
Monitoring of the effectiveness of this E-Safety policy will be undertaken via regular feedback on Safeguarding. The Safeguarding link Governor will review e-safety as part of their remit.

### Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator/Designated Senior Person.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher/Senior Leadership Team are responsible for ensuring that the E-Safety Coordinator/Designated Senior Person and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator/ Designated Senior Person.

## E-Safety Coordinator/Designated Senior Person:

- leads on e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

## Network Manager:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ E-Safety Coordinator/Designated Senior Leader for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in school policies.

## Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and comply with the Staff Acceptable Use Agreement .
- they report any suspected misuse or problem to the Headteacher/E-Safety Coordinator/Designated Senior Person for investigation/action/sanction.
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the e-safety and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Child Protection/Safeguarding Designated Person:

The Child Protection/Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

## Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good e-safety practice when using digital in and out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school.

### Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- access to parents' sections of the website/VLE and on-line student records.
- their children's personal devices in the school (where this is allowed)

# Policy Statements

## Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of ICT/PSE/other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – parents/carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers.

## Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator/Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

## Training – Governors:

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

## Technical – infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.  It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential incident/security breach to the relevant person, as agreed.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
- Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department.
- Users may use the following types of removable media for the purposes detailed:
    - ✓ CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
    - ✓ USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
    - ✓ Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

## Bring Your Own Device (BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.

- Regular audits and monitoring of usage will take place to ensure compliance.
- Any loss or theft of the device will be reported.

## **Use of digital and video images**:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Student's work can only be published with the permission of the student and parents or carers.

## Data Protection:

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

## Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.
- All staff must comply with the school’s Electronic Communications Policy.

## Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly. All use of Social Media should comply with the school's Electronic Communications Policy.

## Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.
They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
All staff should receive a copy of the E-Safety Policy. The school's Acceptable use Agreement will appear each time a member of staff logs on, they will need to accept the terms of this agreement in order to use network facilities.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established

## In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Safeguarding and Child Protection Policy or Disciplinary Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

## Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

## In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- If a child is found to be misusing the internet by not following the Acceptable Use Agreement, parents/carers will be contacted to explain the reason for suspending the child or young person's use for a particular lesson or activity.

- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they should report this to an adult. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

## Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures.
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action.
    - If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:
        - incidents of ‘grooming’ behaviour.
        - the sending of obscene materials to a child.
        - adult material which potentially breaches the Obscene Publications Act.
        - criminally racist material.
        - other criminal conduct, activity or materials.
        - isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

APPENDIX 1

## Secure transfer of data and access out of school

QEHS recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.
- The school will only release personal data if the request has appropriate legal backing.

APPENDIX 2

**To be retained by Parent / Carer**

# Ysgol Uwchradd Y Frenhiness Elisabeth

## Queen Elizabeth High School

Heol Llansteffan,
Tre Ioan,
Caerfyrddin,
Sir Gaerfyrddin,
SA31 3NL

01267 245300

Llanstephan Road,
Johnstown,
Carmarthen,
Carmarthenshire,
SA31 3NL

01267 245300

# Gwybodaeth Cartref Ysgol

## Home School Information

## OUR VISION

As a school, we recognise that education is not a rehearsal. It is a one-time chance for your children and we feel deeply our responsibility both to them and to you. What we strive very hard to do, therefore, is to educate in the true sense of the word, to ‘draw out’ the immensely varied potentialities of all the pupils we have to privilege to serve. We aim to do that by the excellence of our work in the classroom, in our extra-curricular provision and in our pastoral care. To achieve these goals we need to work in partnership with you as parents and carers, as explained in this Home School Agreement.

We should be grateful if you would take the time to read it, sign it and return it to us.

## ATTENDANCE

We can only help your children as you and they have every right to expect if they are in school. So we (and the law of the land) take pupil attendance very seriously. We do expect your full support in ensuring that your children come to school regularly and on time. Absence, however good the reason, is still absence and it has its cost in terms of ground lost in the course of study. ‘Catching up’ can never fully replace missed lessons.

There will, of course, be times when children cannot attend – when they are ill, for instance. In such cases it helps us enormously if we are told on the first day of absence and we would ask you to make every effort to do this. You can,

- phone the school on 01267 245366
- e-mail – the attendance officer - adavies@qehs.carms.sch.uk

If this is somehow not possible, we would ask you to either send a note with your child on their return to be given to the form tutor or make a note in your child’s planner for the form tutor to see. In all cases we must be told the reason for the absence.

In cases where the absence is known in advance we would ask you to inform us as soon as possible. We would also urge you to avoid, as far as possible, booking medical or dental appointments for your children in school time. The same applies to taking family holidays during term time, which also needs the permission of the Headteacher. While we do understand the pressures that may lead to this, the loss of teaching time is serious and will probably have an effect on your children’s progress.

We would also point out, politely but clearly, that reasons for absence must be valid and reasonable. We cannot accept explanations such as ‘shopping’, ‘private entertainment’ or ‘visiting relations’.

In the rare cases when our concerns over a pupil’s attendance become sufficiently serious, we will have to inform the Education Welfare Officer who will then pursue the matter as far as necessary to resolve the problem.

## USING COMPUTERS IN SCHOOL

Computers and other IT devices are now central to school life and to the way we deliver lessons. They have brought enormous advantages but also, as you will know from home computer use, certain risks. To minimise the risks, and to protect all our pupils, we have a code of conduct for computer use in school which we strictly enforce. It is as follows:

- pupils can access the computer system only through their own usernames and passwords, which they should not share with anyone else;
- once logged on, pupils should use the computer for legitimate educational purposes only;
- all copyright laws and intellectual property rights must be respected;
- pupils are responsible for any e-mails they send, which should be worded appropriately;
- pupils are not allowed access to public chat rooms;
- pupils are not allowed to send anonymous messages or chain letters;
- pupils should not attempt to download and/or install any software themselves on to the school's system, even 'free' software, which often carries hidden viruses or cookies.

In the interests of all, the school does monitor all computer use within the building. We take very seriously any inappropriate or irresponsible use of our computer system by any pupil. If the circumstances warrant it, we reserve the right to withdraw a pupil's access to the system. Very serious cases may even result in external legal action.

## PHOTOGRAPHY, FILM AND VOICE RECORDING

From time to time we may wish to photograph, film or voice-record your children. We will only ever do this for educational purposes.

If these crop up in the course of day-to-day curriculum activities your permission is generally not legally required but we will not pressurise any pupil into this who does not wish to be recorded. We will also respect your wishes if you tell us that you do not wish your child to be recorded, though it will not always be possible to let you know in advance.

If we wish to record your child for reasons other than the delivery of the curriculum, we do need your permission and we will do nothing without it.

## UNIQUE LEARNING NUMBER (ULN) NOTIFICATION

The information you supply will be used by the Chief Executive of Skills Funding, to issue your child with a Unique Learner Number (ULN), and to create a Personal Learning Record.

*Details of how your information is processed and shared can be found at http://bit.ly/bmHWNp*

# HOME SCHOOL AGREEMENT

This is included in the Pupil Planner. Pupils, Parents/Carers and Form Tutors are asked to sign this agreement at the beginning of each academic year.

**The school promises to:**

- provide a broad, balanced education;
- have high expectations, helping pupils to achieve their potential;
- keep high standards of teaching, support and guidance;
- set regular and appropriate homework;
- mark and monitor work regularly;
- check and sign the planner regularly;
- provide written and verbal reports about progress;
- make opportunities to discuss progress, including Parents' Evenings;
- provide pupils with a safe, well-disciplined working environment;
- encourage pupils to have a good, responsible attitude towards their physical, mental and moral health;
- offer a wide range of activities outside the classroom;
- deal quickly and properly with any matters of concern and, where appropriate, refer matters on to other agencies;
- make every effort to protect the identity of children.

**Pupils promise to:**

- attend school regularly and be punctual at all times;
- work with concentration and effort;
- complete homework on time and to the best possible standard;
- bring the appropriate basic equipment to lessons;
- wear the correct school uniform;
- share responsibility for the school environment;
- keep to the school rules and behave responsibly when in school or travelling to and from school;
- look after school property;
- remain on school premises during school hours unless given permission to leave;
- treat all members of the school community as well as the school environment with consideration and respect.

**Parents/carers promise to:**

- ensure good standards of attendance and punctuality and inform the school promptly about any reasons for absence;
- encourage and support homework;
- supervise homework and provide suitable conditions for it;
- read, check and sign the Planner every week;
- attend Parents' Evenings and school functions;
- make sure that proper school uniform is worn;
- provide basic equipment such as a well-stocked pencil-case, dictionary and calculator and make sure they are brought to school;
- make sure that items such as ingredients for practical lessons and P.E. kit are available when needed;
- make sure that lost or damaged books and equipment are replaced;
- support the school's policies;
- where appropriate, inform the school of any concerns about a child's behaviour out of school;
- inform the school promptly of any changes in home circumstances.

APPENDIX 3

# Ysgol Uwchradd Y Frenhines Elisabeth

## Queen Elizabeth High School

Heol Llansteffan,
Tre Ioan,
Caerfyrddin,
Sir Gaerfyrddin,
SA31 3NL

01267 245300

Llanstephan Road,
Johnstown,
Carmarthen,
Carmarthenshire,
SA31 3NL

01267 245300

# Gwybodaeth Cartref Ysgol

## Home School Information

Pupil Name: ______________________ Form: ______

Dear Parent/Carer

In order for our home school links to be efficient, we need accurate pupil data, such as updated mobile numbers, and email addresses in particular.

Although you may previously have provided this information, we are aware and conscious of the fact that some of it may be out of date. I therefore respectfully ask that you complete the attached data capture form.

In addition to this, the school entry system has recently been updated to accept biometric information for access into the school building. In order for us, as a school to comply with The Protection of Freedoms Act 2012, it is necessary for us to seek your written consent before we take your child's/children's fingerprint. I therefore ask that you complete the attached form and return it to us at your earliest convenience.

Yours sincerely

Mr P Spencer

Headteacher

Annwyl Riant/Warcheidwad

Er mwyn i'r cysylltiadau rhwng y cartref a'r ysgol i fod yn effeithiol mae angen data cywir arnom, e.e rhifau ffôn symudol a chyfeiriadau ebost yn arbenning.

Er eich bod wedi darparu'r wybodaeth eisoes, rydym yn ymwybodol bod peth ohono yn anghywir erbyn hyn.  Gofynnaf yn garedig i chi lenwi'r ffurflen hon.

Yn ychwanegol at hyn, mae system mynedfa'r ysgol wedi ei diweddaru er mwyn derbyn gwybodaeth biometrig i ganiatau mynedfa i'r adeilad.  Mae angen i ni gael eich caniatâd cyn i ni allu cymryd ol bys eich plenty at y diben hwn.  Gofynnaf felly i chi lenwi'r ffurflen â'i dychwelyd cyn gynteg ag y bo modd.

Yn gywir

Mr P Spencer

Pennaeth

## Notification of intention to process learners' biometric information

- **Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them.**
- **Queen Elizabeth High School intends to take and process learners' biometric information. This information will be used as part of an automated biometric-recognition system, which measures physical characteristics in order to identify or recognise individuals. The system will store information which digitally represents measurements relating to your child's fingerprint.**
- **Queen Elizabeth High School WILL NOT use the biometric information for any purpose other than that stated above. Queen Elizabeth will store the biometric information collected securely and will not share this information with any third parties other than the service provider of the door access system.**
- **If you do not wish your son's/daughter's biometric information to be processes by the school, we will provide reasonable alternative arrangements that allow him/her to access the building.**
- **You can object, in writing, to the proposed processing of your child's biometric information at any time or, if you consent, you can withdraw this consent at any time but must do so in writing (as per the address below).**
- **Your son/daughter may at any time object or refuse to allow their biometric information to be used even if you have given your consent. We will provide reasonable alternative arrangements that allow him/her to access the building. Please ensure you explain this to your child.**
- **When your son/daughter leaves school, or if for some other reason he/she ceases to use the biometric system, his/her biometric data will be deleted.**
- **Further information and guidance can be found via the following links:**
- **-ICO guidance on biometrics in schools 2008**

**www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_finger_view_v1.11.pdf**

**-ICO guide to data protection**

**www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx**

**PARENTAL CONSENT FOR: USE OF BIOMETRIC DATA**

Please sign and date the form below if you agree your child's biometric information (as described above) can be used by Queen Elizabeth High School to allow your child to gain access into the school building and register for our cashless catering system:

Full name of child: ___________________________ (PRINT)

Current year group: ____________________

Name of parent/carer: __________________________ (PRINT)

Signature of parent/carer: _____________________

Date: ___13/7/15______

# Admissions Form

**Confidential**

All schools are required by law to keep on record details of students admitted, therefore, be grateful if you would fully complete this form and return to the school as soon as possible.

**PLEASE COMPLETE THIS FORM IN BLOCK CAPITAL LETTERS**

| | | | |
|---|---|---|---|
| **Student Details:** | | | |
| Legal Surname | | Legal Forename | |
| Middle Name | | Gender | |
| Form | | Date of Birth | |
| Home Address | | Home Phone Number | |
| Post Code | | | |

| | |
|---|---|
| **Details of Previous School (s)** | |
| School Name / Address | Contact Number |
| | |
| | |

| | | | |
|---|---|---|---|
| **Details of those with legal responsibilities:** | | | |
| **Parent / Carer 1** | **Relationship (eg. Father, Mother etc)** | | |
| Title | Dr / Mr / Mrs / Miss / Ms / Other | Parental Responsibility | Yes / No |
| Name: | | Surname: | |
| Mobile Phone: | | E-Mail Address: | |
| Place of Work | | Job Title | |
| Works phone number | | | |

| | | | |
|---|---|---|---|
| **Details of those with legal responsibilities:** | | | |
| **Parent / Carer 2** | **Relationship (eg. Father, Mother etc)** | | |
| Title | Dr / Mr / Mrs / Miss / Ms / Other | Parental Responsibility | Yes / No |
| Name: | | Surname: | |
| Mobile Phone: | | E-Mail Address: | |
| Place of Work | | Job Title | |
| Works phone number | | | |

| | | | |
|---|---|---|---|
| **Parents' details (if not the same as the student):** | | | |
| **Relationship (eg. Father, Mother etc)** | | | |
| Title | Dr / Mr / Mrs / Miss / Ms / Other | Name: | |
| Surname: | | Home Number: | |
| Mobile Phone: | | E-Mail Address: | |
| Address: | | Post Code | |
| Parental Responsibility | Yes / No | Court Order | Yes / No |

| | | | |
|---|---|---|---|
| Correspondence | Yes / No | Do you require a pupil report to be sent to this address | Yes / No |

OTHER CONTACTS

| | | | | |
|---|---|---|---|---|
| **Other Contacts in an emergency *(in order of preference)*** | | | | |
| | Name | Home Phone Number | Mobile Number | Relationship to Pupil |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |

| | | | |
|---|---|---|---|
| **Brothers / Sisters in this School** | | | |
| Name | Form | Name | Form |
| | | | |
| | | | |

MEDICAL INFORMATION

| | | | |
|---|---|---|---|
| **Doctor Details** | | | |
| Surgery Name | | Surgery Address | |
| Surgery Telephone Number | | | |

| |
|---|
| **IMPORTANT MEDICAL INFORMATION I.E. ASTHMA / EPILEPSY** |
| |

| | | |
|---|---|---|
| **Do you give consent for your child to receive emergency medical treatment?** | **Yes** | **No** |

## NATIONAL IDENTITY

Welsh □ English □ Scottish □ Irish □ Other □

## FIRST LANGUAGE SPOKEN AT HOME

Welsh □ English □ Other □

## ETHNICITY

### (a) White

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| British | □ | Traveller of Irish Heritage | □ | Gypsy / Roma | □ | Any other white background | □ |

### (b) European

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| White and Black Caribbean | □ | White and Asian | □ | White and Black African | □ | Any other white background | □ |

### (c) Asian or Asian British

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Indian | □ | Bangladeshi | □ | Pakistani | □ | Any other Asian background | □ |

### (d) Black or Black British

| | | | | | |
|---|---|---|---|---|---|
| Caribbean | □ | Any other black background | □ | African | □ |

## WELSH QUESTIONNAIRE

The following questions ask about the pupil's ability in the Welsh language and its use in the home.

1. Can your child speak Welsh? If ***NO***, there is no need to answer questions 2 to 5**.** (Please Delete) Yes / No

2. Fluency in Welsh *(Only answer this question if you answered Yes to Question 1),* Which one of the following statements best describes your child's fluency in Welsh? (Please tick).

| | |
|---|---|
| Speaks Welsh Fluently | |
| Speaks Welsh but not Fluently | |

3. Does your child speak Welsh in the home? Yes / No

4. Does your child speak Welsh at home with parents or guardians? *(Only answer this question if you answered Yes to both questions 1 and 3).* Which of the following best describes the use of the Welsh language by your child at home? (Please tick)

| | |
|---|---|
| Speaks Welsh with one parent or guardian only | |
| Speaks Welsh with both parent(s) or guardian(s) only | |
| Does not speaks Welsh at home with parents or guardian(s) | |

5. Does your child speak Welsh in the home with his or her siblings? *Only answer this question if you answered Yes to both questions 1 and 3* Yes / No

## Declaration of Person with Legal Responsibility

I declare the above information to be correct to the best of my knowledge at the time of completion.
I agree to notify the school any changes in my child's circumstances.
I have read the Queen Elizabeth High Schools' prospectus. My child will abide by the rules of the school and I will support in those ways outlined.

Signed: ______________________ Date: ______________________

Name: ______________________ (please print)

## Rules for Responsible Computer Use.

I declare that I have read and accept the terms of the Internet, World Wide Web and e-mails policy:

Signed: ______________________ **(Headteacher)** Date: 13/7/2015

Signed: ______________________ **(Pupil)** Date: ______________________

Signed: ______________________ **(Parent/Carer)** Date: ______________________

## Parental Consent Form – Publicity of Photographs, Video and Voice

Queen Elizabeth High School and Carmarthenshire County Council occasionally takes photographs or film of pupils. These images are used to demonstrate or promote activities relating to the school, and may include publication in local/national newspapers, websites and social media (such as Facebook, Twitter, Youtube and Flickr).

Use of video and voice recording as part of day to day curriculum activities for teaching purposes generally does not need permission from parents.

It is also important to note that in accordance with national guidelines on the use of photographic images in school, the identity of the individual students will not be revealed on images published by the school.

Please tick the relevant box below:

I **give** permission for my child to be photographed/filmed as detailed above. □

I **do not give** permission for my child to be photographed/filmed as detailed above □

Name and form of pupil: ______________________

Signed: ______________________ (Parent/Carer)

Date: 13/7/15

## Home School Agreement

I declare that I have read and accept the terms of the home School Agreement:

Signed: ______________________________ **(Headteacher)** Date: 13/07/2015

Signed: ______________________________ **(Pupil)** Date: ______________________________

Signed: ______________________________ **(Parent/Carer)** Date: ______________________________

## Data Protection Statement

The purpose of this form is to collect data for further processing within the School/Local Authority Systems. Your signature on this form implies your consent for the school/local authority to process the data. The data will be processed in accordance with the purposes notified by the school/local authority to the Data Protection Commissionaires office and are subject to the Data Protection Act 1998. The information will be entered onto a computer and will form part of the Local Authority School Database.

## **IMPORTANT**

**Please inform the school immediately of any change in your circumstances during the course of the year.**

## New Policy Announcement: Bring Your Own Technology (BYOT) Pilot at Queen Elizabeth High School (Years 12/13)

Dear Parent / Carer,

As you are aware, modern technology is developing at quite a pace, and Queen Elizabeth High School believes that it is important to educate our students about these important developments. Research has shown that using such digital technologies in education can help encourage creativity, motivate and enthuse students, as well as improve communication and team-working skills.

Part of our ongoing IT strategy at Queen Elizabeth High School is to promote and support the use of new technology within our educational environment to aid learning. The school has decided to allow Years 12 and 13 students to **bring in their own tablets/laptops and devices** and gain access to the school's Wi-Fi network. This is a voluntary opt-in scheme and we do not expect parents / carers to purchase new equipment as a consequence.

We are also aiming to pilot social media as an educational tool, as it has the possibility to enrich the learning experience by allowing students and teachers to connect and interact in new, exciting ways. We therefore also ask you to give permission for your child to use external web applications such as (but not restricted to) 'HWB+' and 'Office 365' and to give permission for him/her to create digital content and to allow us to publish such digital content online.

Within this BYOT Information Pack you will find:

3) A series of questions and answers about BYOT programme at Queen Elizabeth High School.
4) A 'BYO User Acceptance Policy' that you must sign, along with your son/daughter, before he/she is permitted to use devices in lessons.

The safety and welfare of our students is of paramount importance to us and there will be a number of regulations/control measures put in place to promote safe use of technology whilst using the school's Wi-Fi network.

Should you have further questions, please contact me at the school, or you are welcome to e-mail Mr Arwyn Lloyd (elearning co-ordinator) at alloyd@qehs.carms.sch.uk. We will do our best to answer any outstanding queries.

Kind regards

P Edwards
Deputy Headteacher

## Bring Your Own Device (BYOT): Parent / Carer Q & A

### 1. What devices are allowed / not allowed?

The policy is for any device / technology that has the ability to connect to the school's wireless network such as tablets, laptops and smartphones.

### 2. When will this happen?

Immediately! Please sign the User Acceptance Policy and return it to the school as soon as possible.

### 3. How do you control what they see online?

The school has technology that can track, monitor and pick up banned / unsafe websites and block this content on their devices. Although we want students to make the right choices and self-manage their use, we ultimately have technology behind the scenes that will protect them when they use the school network. We also have the ability to block users who abuse the position of trust we place in them whilst using the school Wi-Fi network. **ALL** school network traffic is monitored and logged.

### 4. When would they use it?

Many of our teachers at Queen Elizabeth High School believe that having students bring their own devices could be advantageous to teaching and learning. For example, in language subjects students could use an app to help with their spelling, or the devices could be used intermittently in lessons to research on the web. In summary we see their device as simply part of their 'kit bag' alongside pens / folders / textbooks. Some students will be able to ultimately decide to replace all of these hard tools with virtual ones with textbooks, applications and systems on devices that replicate traditional methods of managing their educational work. In order for students to connect the device, they must join the BYOD Wi-Fi network.

### 5. Is this device insured?

No. The school is allowing access to personal devices. They are not owned by the school so the school's insurance policy does not cover this. **Personal contents insurance *should* cover this device on YOUR OWN policy but please check with your provider that there are no exceptions in your policy.**

### 6. Can I still study adequately without a laptop / device?

Absolutely, the school has many rooms and areas where students can access computers before, during and after the school day. Additionally, quality learning can take place without the need for technology. This is an opt-in scheme, where students feel more comfortable with technology they can use. However, traditional approaches to learning are still appropriate and, importantly, work.

# Queen Elizabeth High School Bring Your Own Technology (BYOT) Acceptable Use Policy (AUP)

## What is a Personally Owned Device?

A personally owned device is any device / technology that has the ability to connect to the school's wireless network such as tablets, laptops and smartphones. **All students must sign a copy of this AUP before they can use their own device in lessons.**

## Expectations:

The school has set out below the expectations of students using their personally owned devices. Each expectation shall apply to students when they are in or around the school. Misuse of a device will result in the device being banned from the school network. Students will:

√ only use appropriate technology at the teacher's discretion

√ be aware that the school is not liable for loss, damage, misuse, or theft of personally owned devices brought to the school even if left in locked rooms

√ use their device for <u>educational purposes only</u>

√ only use appropriate educational applications and / or programmes on their device

√ only access appropriate educational files on their device

√ observe all school internet filters

√ only access the network using the provided wireless network

√ use headphones when listening to audio files such as music on their device so that the volume should be kept at a level that doesn't disrupt others. When in the classroom, students may only listen to audio files when given permission by their teachers

√ follow copyright laws concerning illegal copying of music, games, movies and other protected works

× not bring desktops or towers to school

× not connect their devices to the local area network via an Ethernet cable

× not use any device as a cyber – bullying tool

× not be allowed to use gaming consoles or gaming devices to connect to the network

× be prohibited from taking pictures or digital recordings of staff or students without their prior written permission. The distribution of such media may result in exclusion or criminal charges

× never share your passwords with other students or staff

× must not use devices in such a way as to cause a disturbance on school premises

**Educational Purposes**

Students will use their electronic device for educational purposes only. This may be in a classroom activity, such as researching a topic, using a calculator, creating maps, note taking, planner / calendar, document creation or connecting to electronic resources provided by the school. Students are responsible for their personal devices

**Inappropriate communication:**

Students shall refrain from using their device for inappropriate communications. These include but are not limited to the following: bullying, threatening, obscene, profane, vulgar language and / or images that may cause damage to an individual or the school. Students must not use their devices for personal attacks on other students or staff. Students are not allowed to harass or stalk other students or staff. If a student is instructed to stop sending electronic communications they must stop immediately.

**Security**

The school provides content filtering for student access to the internet. However at times, inappropriate material may get past the filters and be viewed by students. Students must report such occurrences to their teacher or administration. Students will be held accountable for any deliberate attempt to bypass the school's filters and security. The school strongly recommends that devices and cases are personalised to prevent loss.

**Social / Web Tools / Collaborative Content**

As a school that recognises the benefits that collaboration brings to education, Queen Elizabeth High School may provide students with access to websites or tools that allow communication, collaboration, sharing and messaging among users. All school rules apply to online behaviour.

**Supervision and Monitoring**

School and network administrators and their authorised employees monitor the use of information technology resources to help ensure that users are secure and conform with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any students or other person, or to protect property. They may also use this information in disciplinary actions, and can provide evidence of crime to law enforcement. If necessary or if required to do so. The school also reserves the right to limit the time of access.

**Technical support and network connections:**

Students who cannot access the wireless network or may have technical issues with their technology tool need to resolve this issue by working with the user manual that came with the device contact the (re)seller directly. These are not school owned devices and the school are unable to allocate resources to troubleshoot connection issues.

**Charging and Printing:**

It is the Students' responsibility to bring their devices to school charged. We are not currently able to offer direct printing facilities. In order to print, work should be placed on the 'My Documents' area of their school account (e.g. by transferring work via USB) and accessed through a school networked PC or use HWB/Office 365/One drive.

### Violations of Acceptable Use Policy

Bringing your own device is a privilege and not a right. Students not following expectations for use of personal devices will face disciplinary action and lose the privilege to utilise personal devices in the school for a period of time, or permanently.

### Use of students' digital images/work

As part of this scheme, students' images or work may be used on the internet. We will ensure that images that include students will be selected carefully and students' names will NOT be used in association with photographers. Any parent / carer who does not wish for their child's image or work to be used in this educational manner should contact the Heads of Sixth Form:
Mrs Lisa Jones (Year 12) ljones@qehs.carms.sch.uk and Mr Jason Killingsworth (Year 13) jkillingsworth@qehs.carms.sch.uk.

## STUDENTS AGREEMENT

I hereby agree to the above Acceptable User Policy for BYOT at Queen Elizabeth High School, and agree that any violation of this AUP will result in intervention. I also agree to manage my device appropriately, and to adhere to the current school internet usage policy.

***I have read and understand the BYOT Acceptable Use Policy, and agree to adhere to the terms and conditions***

**(Student's Name)** **(Form)** **(Student's Username)** **(Student's Signature)**

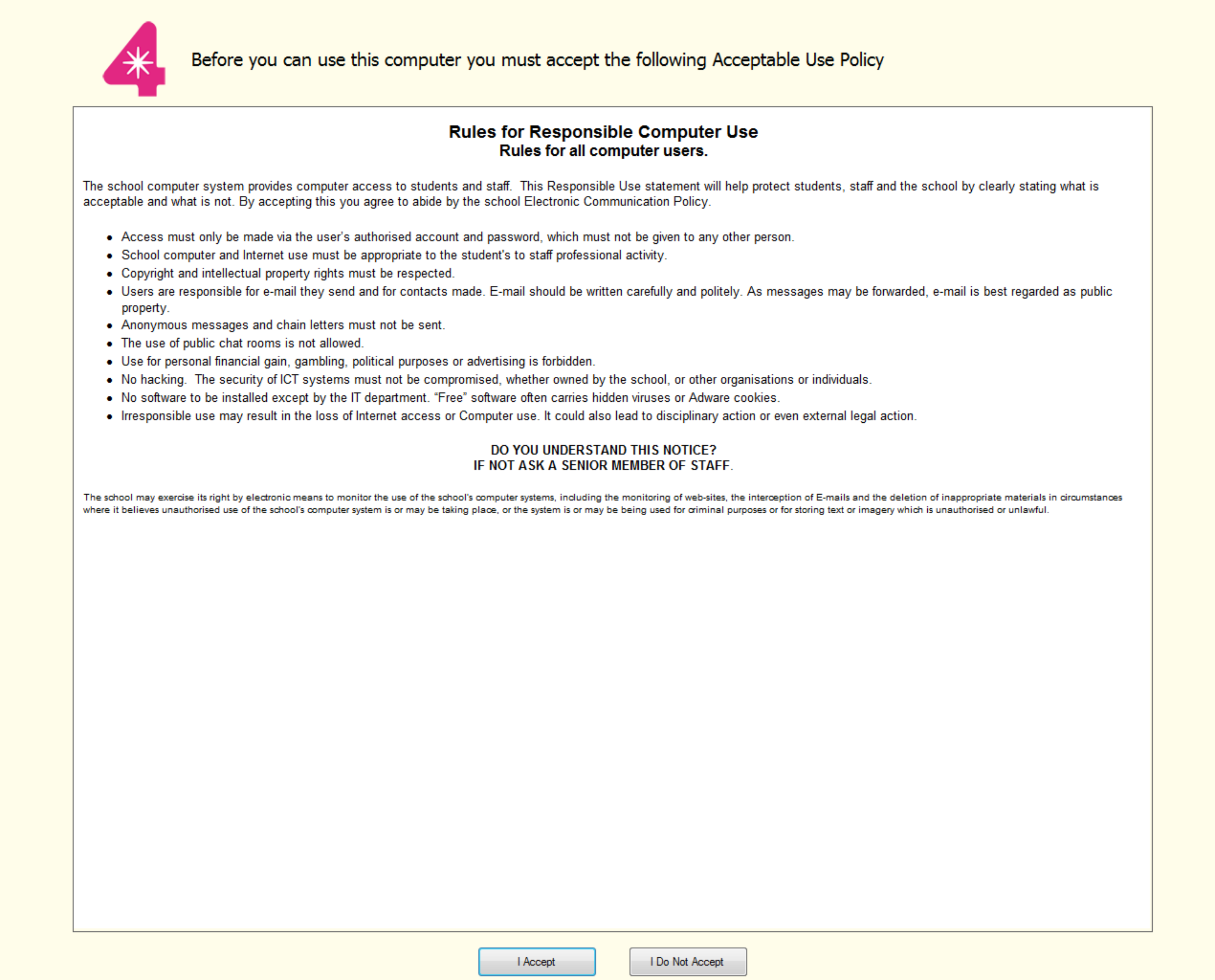
## Parent / Carer Agreement

As part of this BYOT pilot, we are eager to hear parents' / carers' opinions about these developments. Please use the space provided below to share your comments (**positive and / or negative**) with us:

*I have read and understand the BYOT Acceptable Use Policy and I accept the Terms and Conditions within the AUP. I also agree to my child using web based applications as part of this programme.*

**Parent / Carer (Printed)** **Parent / Carer (Signature)**

# APPENDIX 4



Before you can use this computer you must accept the following Acceptable Use Policy

## Rules for Responsible Computer Use
### Rules for all computer users.

The school computer system provides computer access to students and staff.  This Responsible Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not. By accepting this you agree to abide by the school Electronic Communication Policy.

- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's to staff professional activity.
- Copyright and intellectual property rights must be respected.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms is not allowed.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- No hacking.  The security of ICT systems must not be compromised, whether owned by the school, or other organisations or individuals.
- No software to be installed except by the IT department. "Free" software often carries hidden viruses or Adware cookies.
- Irresponsible use may result in the loss of Internet access or Computer use. It could also lead to disciplinary action or even external legal action.

DO YOU UNDERSTAND THIS NOTICE?
IF NOT ASK A SENIOR MEMBER OF STAFF.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.