TALBOT HEATH SCHOOL *"Honour Before Honours"*

# ICT, MOBILE EQUIPMENT AND DIGITAL CITIZENSHIP POLICY

**Date adopted:** 13 October 2026

**Date for next adoption:** Autumn 2027

**Reviewed by:** FGB

**OVERVIEW OF POLICY**

**1. Roles and responsibility**
**2. Communicating School policy**
**3. Making use of ICT and the Internet in School**
**4. Learning to evaluate Internet content**
**5. Managing information systems**
**6. Emails**
**7. Published content and the school website**
**8. Mobile phones and personal devices**
**9. Cyberbullying**
**10. Managing emerging technologies**
**11. Protecting personal data**
**Appendix – acceptable use policy**

## Introduction

The school recognises that ICT and the Internet are excellent tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff, parents and visitors use it appropriately and practise good digital citizenship. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

Digital Citizenship covers the Internet but it also covers mobile phones, portable devices and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of Digital Citizenship falls under this duty. It is important that 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 is an aid in regulating ICT activity in school and provides a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Digital Citizenship is a whole-school issue and responsibility.

Cyber-bullying by students is treated as seriously as any other type of bullying and is managed through our Anti-Bullying Policy and Procedures. All incidents of sexting are followed up and dealt with by the DSL/DDSL following guidelines from UKCCIS.

This Digital Citizenship policy is designed to safeguard our students and develop their resilience when using technology (see Digital Citizenship curriculum programme).

This policy is reviewed annually on an official basis, as well as ad-hoc minor changes and updates which are implemented as advised by governing bodies and specialist advisory organisations to ensure ongoing effectiveness of the policy.

## 1. Roles and responsibility

The Headteacher and Governors ensure that the Digital Citizenship policy is implemented and compliance with the policy monitored, but the day-to-day management of digital citizenship in the school is the responsibility of the IT Team who work closely with the SLT in this regard.

### Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of digital citizenship (as part of the wider remit of Safeguarding and Child Protection) across the school with further responsibilities as follows:

- The Headteacher informs the Governors at FGB meetings about the progress of, or any updates to, Digital Citizenship and ensures Governors know how this relates to Child Protection.
- The Governors must ensure Child Protection includes an awareness of digital citizenship and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Safeguarding guidance and practices are embedded.
- The Headteacher ensures that staff are trained in online safety and updated when necessary.
- The Headteacher ensures that 'Prevent' training highlights the use of the Internet and social media by extremist groups wishing to radicalise young people.

### The Network and E-Learning Managers:

- Ensure that this policy is reviewed annually, with up-to-date information available for all staff to teach Digital Citizenship and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and students. At Talbot Heath a Smoothwall Firewall/Web Filter which is cloud hosted by Bistech is used.
- Ensure that all adults are aware of the filtering levels and why they are there to protect students.
- The IT Lead regularly meets with the DSL to discuss filtering and monitoring and reports any concerns immediately.
- Liaise with the designated safeguarding team so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training according to new and emerging technologies so that the correct digital citizenship information can be taught or adhered to.
- Personal equipment must not be used for work purposes.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Manage/oversee the iPad Management System and operation of the School iPads.

### Individual Staff

- Encourage the use of ICT (including iPad use) within their subject area enhancing the learning experience and the quality of students' work.
- Increase the integration of ICT into their lessons so that ICT will be viewed as just another tool in the equipment provision of the subject area.
- Extend the topics and exploit the opportunities available within the lesson content providing guidance as to the most effective use of ICT including relevant Internet use in particular specific website addresses related to the topics covered.

- Keep up to date with changes in subject specific software and hardware, iPad applications available to schools.
- Support and reinforce the Digital Citizenship guidance delivered through both discrete and cross-curricular sessions, ensuring students are aware of Digital Citizenship guidelines and that they follow this policy.
- Read and adhere to guidance published by the school via the DfE (in particular, references to helpful advice on the use of social media for radicalisation), The UK Safer Internet Centre, UK Council for Child Internet Safety and CEOP (in particular, the 'thinkuknow' website).
- Check that the filtering levels are appropriate for their students and report any concerns to the IT Team.
- Ensure that students are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner, so that they can be in control and know what to do in the event of an incident.
- Use electronic communications in an appropriate way that does not breach the Privacy and Electronic Communications Regulations (PECR) that sit alongside the UK GDPR and the Data Protection Act 2018. Remember confidentiality and do not disclose information from the network, pass on security passwords or leave a computer unattended in a classroom when they or another user is logged in.
- Report accidental access to files/folders as well as inappropriate materials online etc. so that it can be reviewed and resolved and inappropriate websites are added to the restricted list. Similarly, all Staff should report Spam Email (or suspected Spam Email)
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies to a member of the Senior Leadership Team.
- Keep up to date with emerging technology, utilise equipment provided and attend iPad, E-Learning and Digital Citizenship training sessions when possible.

**Form Teachers**

- Support the ICT Department in ensuring students receive important information, and work with them to ensure regular checks and updates are performed as well as displaying associated information.
- Ensure students are aware of digital citizenship guidelines and to act as a point of contact if students have any concerns.
- Keep channels of communication open so that students can discuss any concerns or issues regarding digital citizenship.

**Head of Faculty/Junior School Subject/ Key Stage Co-ordinator**

- Take full advantage of the ICT based resources available.
- Ensure that ICT capability is developed throughout the faculty/subject/Key Stage.
- Support staff in their ICT training and professional development.
- Set priorities for the further development of ICT.
- Support other subject areas in the use of ICT within their curriculum.
- Ensure all staff are aware of digital citizenship guidelines and offer support with any issues that may arise.

**Students**

- Take full advantage of the opportunity to develop their ICT skills.
- Use all ICT equipment including iPads solely for the purpose for which it is intended.
- Avoid waste of materials by unnecessary printing and to use the recycling facilities available.
- Follow the school's digital citizenship guidelines and ensure they do not put themselves or others at risk.
- Participate in digital citizenship activities and follow guidelines given.
- Tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand

- Use ICT in line with the Acceptable Use Policy (see appendix)

**Parents/Carers**

- Encourage the acquisition of ICT skills.
- Encourage good use of the ICT facilities in the school and at home.
- Be aware of the dangers of some online related activities and monitor appropriate Internet usage at home.
- Keep channels of communication open so that students can discuss any concerns or issues regarding digital citizenship
- Support the school in its digital citizenship guidance to students and reinforce this at home

## 2. Communicating the policy

This policy is available to all parents, staff and students on the school's website. Rules relating to the School Code of Conduct when online, and digital citizenship guidelines, are displayed around the school. Digital Citizenship is integrated into the curriculum in any circumstance where the Internet or technology are being used, as well as being specifically addressed in the ICT curriculum as appropriate. On joining the school, new Students in Year 3 and above are required to adhere to the relevant sections in this policy, which all staff are also expected to adhere to, in its entirety. Any misuse of the school's ICT equipment will be dealt with using the School's Behaviour and Discipline policy.

## 3. Making use of ICT and the Internet in School

Using ICT and the Internet in school brings many benefits to Students, staff and parents. The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for Students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer, iPad or other electronic devices. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (of any type, including child sexual abuse images)
    - promoting discrimination of any kind
    - promoting racial or religious hatred
    - promoting illegal acts
    - any other information which may be offensive to others within a school environment
- Use the school facilities for running a private business
- Visit sites that might be defamatory or incur liability on the part of Talbot Heath or adversely impact on the image of the school
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information, personal information

    - databases and the information contained therein
    - computer/network/email or other personal passwords or access codes relating to the school systems.

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of malware of any type, and sustained high volume network traffic
- Use the Internet for illegal file sharing or in any other way that could reasonably be considered inappropriate
- Use instant messaging or chat software or websites or access social networking sites without the express permission of their teacher
- Use VPNs or proxy sites, or otherwise attempt to bypass network security in any way
- Make **any** attempt to access the dark/deep web

Expectations of the use of school's ICT facilities outlined in this policy, apply to staff, Students and visitors both in and out of lessons.

Regular staff training addressing online risks will take place as part of the Safeguarding Training programme. Urgent issues will be communicated to staff through staff briefings.
Information will be communicated to parents as necessary.

## 4. Learning to evaluate Internet content

With so much information available online it is important that Students 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. Students will be taught, at age appropriate levels:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
- to acknowledge the source of information used and to respect copyright. The school will take any intentional acts of plagiarism very seriously.

If staff or Students discover unsuitable sites whilst in school then the device used, web address, time, date and content must be reported. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the Senior Leadership Team. Regular checks will take place to ensure that filtering services are working effectively.

## 5. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers, network and Internet filtering as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school Information Systems and user access will be reviewed regularly by the ICT Support team and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any school computers.
- Files held on the school network will be regularly checked for viruses.
- The use of user logins and passwords to access the school network will be enforced.
- IT systems security options are regularly reviewed and enforced and options such as 2FA are used where applicable, as well as spam filtering and domain spoofing enabled.
- Deep inspection is enabled on our firewall/filter and the use of an SSL certificate is implemented to ensure that traffic coming in/out from the Internet is legitimate and not malicious.
- Data Protection/GDPR is regularly reviewed between Talbot Heath School's Data Protection Officer

For more information on data protection in school, please refer to our Data Protection policy, which can be accessed on the school's website. More information on protecting personal data can be found in section 11 of this policy.

## 6. Emails

The school uses email for contacting staff and Students, and externally for contacting parents and other agencies and is an essential part of school communication.
Access in school to external personal email accounts may be blocked. The school has the right to monitor school emails and their content, but will only do so if there is suspicion of inappropriate use.

**School email accounts and appropriate use**

- Staff should only use official school email accounts for school-related matters and contact with other professionals for work purposes. Communication with Students, parents or carers may also require the Headteacher and/or Junior School Head to be copied into these communications. Personal email accounts must not be used to contact any of these people.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff should forward emails from parents expressing a serious concern, along with their replies, so that this information is communicated to the Headteacher and/or Head of Junior School and then noted on the pupil profile in ISAMs.
- 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 line manager or a senior member of staff.
- Staff must tell their manager or a member of the Senior Leadership Team 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.

**Students should be aware of the following when using email in school**, and will be taught to follow these guidelines through the Computing curriculum and in any instance where email is being used within the curriculum or in class:

- All Senior School Students and older Junior School Students (Year 3 upwards) are provided with a school email account and Students may only use approved email accounts on the school provided systems.
- As part of Digital Citizenship, Students are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases will be dealt with accordingly.
- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from users within the school or from an external account. They must not attempt to deal with this themselves.

## 7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting school projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or Students will be published. For information

on the school policy on children's photographs on the school website please refer to section 7.1 of this policy.

A team of staff, under the leadership of the Headteacher are responsible for publishing and maintaining the content of the school website. The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Students should not publish anything on the Internet involving the school unless permission has been granted by the Headteacher.

### 7.1 Policy and guidance of safe use of children's photographs and work

Photographs and Students' work bring our school to life, showcase our students' 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.

Under UK GDPR and the Data Protection Act 2018 images of Students and staff will not be displayed in public, either in print or online, without consent (as per parental contract).

**Using photographs of individual children**

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. This includes the use of mobile devices and cameras across the whole school including the EYFS setting, too.

The school follows general rules on the use of photographs of individual children:

- Consent from parents will cover the use of images in:
    - all school publications
    - on the school website
    - in videos made by the school or in class for school projects.

- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that Students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the Students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child without the written permission from parents. Groups may be referred to collectively by year group or form name.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the Students.
- There are some instances when parents or guardians will be informed they may not take photos or videos for example at events such as swimming or when there are copyright issues for example school productions.

### 7.2 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with school policy.

Students must not take photos or record videos of members of staff or other Students without prior consent and must only be for school purposes.

### 7.3 Social networking, social media and personal publishing

- Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. The school will normally block/filter access to social networking sites via the school network, including via iPads/other electronic devices.
- Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught through the Computing/PSHE curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.
- The school follows general rules on the use of social media and social networking sites in school:
-
    - Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. Students are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
    - Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use, without the risk of inappropriate pop-ups or adverts, where possible.
    - Official school blogs created by students/year groups/school clubs as part of the school curriculum will be moderated by a member of staff.
    - Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.
    - Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through this policy.

## 8. Mobile phones and personal devices

Mobile phone 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 in today's society, 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 students 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. Pictures must never be taken without the express permission of all persons to be photographed.

The school's expectation is that mobile devices will be used responsibly at all times and this pertains to the EYFS setting specifically as much as to the rest of school. Certain measures are taken to ensure that students adhere to this expectation. Some of these are outlined below.

- Students (other than Sixth Formers) are not permitted to use mobile devices, whether they are mobile phones or items such as smartwatches, during the school day.
- In Senior School (years 7-11), all mobile devices (including mobile phones and smartwatches) must be switched off and locked in a Yondr pouch throughout the school day. The Yondr pouch must be placed in a student's school bag.
- Junior School students may not have their mobile phone device with them during the school day. They will ensure that they hand their mobile phones devices into the office for safe keeping on arrival in school and collect at the end of the school day.
- Sixth Form Students are allowed to use their mobile device in the Sixth Form Common Rooms. In other parts of the school, they must not use their mobile device, unless they are working in the Library or Hub, in which case they may use their phone discreetly to listen to music while working.
- Mobile devices are not permitted on school trips in the Junior School. For Senior School trips, mobile devices should be switched off, locked in a Yondr pouch and stored in the student's bag. At the discretion of the trip leader, students may be allowed to unlock their phone at certain times during the trip, for example to advise parents of a late arrival back at school during the return journey.
- The school will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. Banter will not be tolerated or treated as "part of growing up." For more information on the school's disciplinary sanctions read the school's Behaviour and Discipline policy.
- Mobile devices can be confiscated by a member of staff, and the device can be searched by nominated senior members of staff if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Individual students are responsible for their own phones and other mobile devices and should ensure that they take care of them at all times. The normal disciplinary procedures apply in the event of damage to another student's property.
- Headphones must not be worn during lessons unless specific permission is given by the teacher.
- Students must not use iPads to broadcast music or other media unless permission to do so has been given by a member of staff. Other mobile devices should not be used for this purpose during the school day as they will be locked in a Yondr pouch.
- Students must ensure that files stored do not contain violent or pornographic images or other material that is likely to cause offence. In very serious cases the police may be contacted.
- Parents / Guardians should phone either the Junior School or Senior School offices during the school day if they need to contact their daughter.
- It should be noted that power supplies for these devices must not be brought to school as all electrical devices used in the school must be PAT tested.

### 8.1 Mobile phone or personal device misuse

**Students**

- Students who breach school policy relating to the use of personal devices will be disciplined in line with the school's, Mobile Devices and Behaviour and Discipline policies.
- There are clear sanctions in place for students who break these rules, which are outlined in the Mobile Devices policy. Sanctions include immediate confiscation of the phone, after school detention, daily hand in of the device to the school office and temporary exclusion.

- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile device in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body.

**Staff**

- Staff should not ~~to~~ use their own personal devices to contact students or parents either in or out of school time unless in exceptional circumstances.
  This includes School Trips – the Staff member(s) leading the trip(s) is responsible for contacting the ICT Department requesting Mobile Phone(s) for the trip in advance to the event taking place.
- Staff should use school equipment if photos or videos are being taken as part of the curriculum or in a professional capacity, staff should never take photographs of school students or events on their personal device. This includes in the EYFS setting.
- The school expects staff to lead by example. Personal mobile devices should be switched off or on silent during school hours.
- Adults at the premises are not permitted to use their mobile phone or other devices in the areas of the designated EYFS setting during operating hours without permission of the Headteacher. All mobile phone devices must be stored away from the children and only used when children are not present. If staff have wearable devices the smart function must be disabled when working with EYFS children.
- Any breach of school policy may result in disciplinary action against that member of staff.

**8.2 Mobile Equipment Issued by the school**

The purpose of this section is to set out the responsibilities and acceptable use guidelines for all users that are in receipt of a school laptop computer or other mobile ICT items such as mobile phones or iPads.

- Any mobile equipment, accessories, software and operating systems issued to staff or students remain the property of Talbot Heath School Trust Ltd. and are provided on a loan basis. These items can and may be recalled at any time.
- School loaned iPads must have a passcode set, preventing unauthorised access.
- School-provided laptops for Staff must be encrypted to follow GDPR protocol. The ICT Department will do this before handover of the device.
- Staff and students must take personal responsibility for the security of the equipment, software and data in their care. Reasonable precautions to avoid loss or misuse of the mobile equipment should be taken. Any loss or intentional misuse by staff may result in disciplinary action and recovery of any costs incurred by the school. Staff and students must refrain from leaving ~~a~~ mobile equipment in an unattended vehicle at all times.
- Students and parents will be expected to sign the school's acceptable use agreement, further down in this policy.
- Staff and students must only use the equipment for personal use as long as it does not interfere with, or conflict with, school use. Staff are responsible for exercising good judgment regarding the reasonableness of personal use. Students should seek the advice of the ICT department or their Form Tutor.
- A register of all mobile equipment issued to students and staff will be held centrally by the school.
- Students should not use school issued iPads for non-educational purposes whilst at school and at home.
- Homework may be set which will require the use of their iPad at home, however it is important that Students do not use their iPad excessively at home and it is charged overnight in a family room. Its primary use is as a Teaching and Learning device and students should try to limit the amount of time that they spend using the iPad. If students have been spending a large amount of time doing their homework on the iPad, they should ensure that they take regular breaks.

- Under EYFS regulations technology is used to enrich learning experiences and support children's development. Screen use must be purposeful, age-appropriate and enhance learning outcomes. In line with current guidance, children will not engage in prolonged periods of screen use and, where screens are used, this will be limited to short, focused activities with a maximum limit of 1 hour a day. Screen use does not replace play, outdoor learning, physical activity or meaningful interactions with adults and peers. Staff support children in developing safe and responsible habits around technology and work in partnership with parents to promote healthy screen use
- 
- All the guidelines detailed in Sections 8 and 8.1 apply.

## 9. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies to prevent and tackle bullying are set out in the school's Anti-bullying policy. The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

## 10. Managing emerging technologies

Technology is progressing rapidly and new 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 benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

## 11. Protecting personal data

The school believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of ~~the~~ how data is collected, what is collected, and how it is used. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the well-being and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

This may include registering pupil details with relevant digital platforms to support learning. Parental and pupil consent is given by default for such data to be processed accordingly in line with the Online Safety Act and current GDPR regulations.

In line with the UK GDPR and the Data Protection Act 2018, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary;

- process the data in accordance with the data subject's rights;
- ensure that data is secure;
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection read the school's data protection policy and for issues relating to safeguarding, read the safeguarding policy and procedures. The Designated Safeguarding Lead in the school is responsible for safeguarding throughout the whole school including the Early Years Foundation Stage.
The NSPCC Whistleblowing Advice Helpline 0800 800 5000 offers free advice and support to professionals with concerns about how child protection issues including digital citizenship are being handled in school.
The DSL has access to both the early help team who work with children who may benefit from additional external agency input and the Children Services team who deal with concerns for children in need or at risk.

**12. Evaluation**

The effectiveness of the policy is evaluated annually by reviewing the number and nature of incidents across the whole school relating to digital citizenship. Pupil surveys are also conducted regularly and the results analysed.

**Related Documents:**

Safeguarding Policy and Procedure
Anti-Bullying Policy
Acceptable Use Policy (AUP) for ICT
Behaviour and Discipline Policy
Data Protection Policy
Staff Disciplinary Policy
iPad Agreement (Students/Parents/Staff)
Staff Code of Conduct
Whistle-blowing Policy

**Other useful resources:**

UK Council for Child Internet Safety (UKCCIS): Sexting in schools and colleges
DfE: How Social Media is used to encourage travel to Syria and Iraq
www.saferInternet.org.uk https://ceop.police.uk www.thinukuknow.co.uk
https://www.nen.gov.uk/ www.nspcc.org.uk

# APPENDIX:

**ICT Acceptable Use Policy**
The computer network is owned by the school and may be used by students to further their education, and by staff to enhance their professional activities. This policy will help protect all parties by clearly stating what is deemed acceptable and what is not.

The ICT Acceptable Use Requirements cover the security and use of all Talbot Heath School's information and other IT equipment - Including the use of Mobile Devices, Tablets such as iPads, and other electronic communication technology in the school. It also includes the use of Email, Internet, Database(s), Management Information System(s) and Voice communication methods. These requirements apply to all Talbot Heath School staff, students, visitors and parents (hereafter referred to as 'individuals').

These requirements apply to all information, in whatever form, relating to Talbot Heath School and to all information, handled by Talbot Heath School, relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Talbot Heath School or on its behalf.

Email, Network and Internet access are provided as a tool for educational purposes only. All information files remain the property of the School. You are responsible for the content of your workspace and for ensuring nothing unsuitable or inappropriate is stored there. You must inform the IT Team if you receive an email from someone you do not know or if you receive Spam – or 'suspected to be' Spam to your school Email account.

The use of blogs and podcasts offer opportunities for you to enhance your learning. Teachers may incorporate email, instant messaging, blogs, podcasts, video sharing, online collaborations, virtual learning environments or other technologies as part of their teaching. However, you must not use instant messaging (e.g. WhatsApp, Facebook Messenger, Snapchat etc.), chat sites or social networking sites (e.g. Facebook, Instagram, Pinterest etc.) at school unless you have received express permission from your teacher. You should never publish specific or detailed private thoughts.

**Computer Access Control – Individual's Responsibility.**

Access to the Talbot Heath IT network and systems are controlled by the use of a Username and Password. All Usernames and Passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Talbot Heath IT network systems.

**Individuals must not:**

- Allow anyone else to use their Username and Password on any Talbot Heath IT system (PCs, Email, Management Information Systems, Databases or Other).
- Leave their user account logged in at an unattended and unlocked computer/iPad/other IT system.

Use someone else's Username and Password to access Talbot Heath's IT systems (PCs, Email, Management Information Systems, Databases or Other).

- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Talbot Heath's IT systems or data held.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific need to interrogate the system or data.
- Store Talbot Heath-owned data on any unauthorised (e.g. a personal laptop) equipment (including memory sticks/external storage that are not encrypted)
- Give or transfer Talbot Heath School data or software to any person or organisation.

outside of Talbot Heath School without the authority of a member of the SLT from Talbot Heath School.
- Store personal files such as music, video, photographs or games on Talbot Heath School's IT equipment.
- Attempt to move or relocate heavy IT equipment or connected peripherals that conduct an electrical current.
- Attempt to remove the side panel(s), chassis, or in-built hardware from the computer (both internally and externally).
- Consume or have/leave food and/or drink near the computer systems.
- Intentionally cause damage to the computer systems.
- Transfer data with personal staff/student information on an unencrypted storage device.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

All individuals **must** report any concerns with the computer equipment, peripherals, network or other IT-related queries to the ICT department via the following methods:

- Email: techsupport@talbotheath.org
- Dial: Extension:
  243 – ICT Technician
  306 – IT Department

Report in person at the ICT Office (Located in the room next to Food Tech)

**Internet and Email Conditions of Use**

Use of Talbot Heath School's Internet and email facilities are intended for educational and business use only.

All individuals are accountable for their actions on the Internet and email systems.

**Individuals must not:**

- Use the Internet or email systems for the purposes of harassment or abuse.
- Visit Internet sites, make, post, download, upload, or pass on material, media, remarks, proposals or comments that contain or relate to:
  - Pornography **of any type** (including child sexual abuse images or videos).
  - Promoting discrimination of any kind.
  - Promoting racial or religious hatred.
  - Promoting illegal acts.
  - Any other information which may be offensive to others within Talbot Heath School's environment.
  - Gambling
  - Radicalism
  - Weaponry
- Use profanity, obscenities, or derogatory remarks in communications.
- Use the Internet or email systems to make personal gains or conduct a personal business.
- Use the Internet or email systems to gamble.
- Use the Internet or email systems for illegal File Sharing (or in any other way that could reasonably be considered inappropriate).
- Use the email systems in a way that could affect its reliability, effectiveness or reputation, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Talbot Heath School, alter any information about it, or express an opinion in the name of Talbot Heath School, unless they are specifically authorised to do this.
- Send unprotected, sensitive or confidential information externally.

- Make official commitments through the Internet or email on behalf of Talbot Heath School unless authorised to do so.
- Download or share copyrighted material such as music media files (e.g. mp3), film and video files (of any file type) without appropriate consent.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses or other malware, and sustained high volume network traffic.
- Use VPNs, proxy sites, Mobile Internet Dongles (e.g. 3G/4G/5G Dongles), hotspot from a mobile device or otherwise attempt to bypass network security in any way (this includes the prohibition of "portable browsers" such as Mozilla Firefox or Opera Portable, and the use of Tor – or other alternatives of this software).
- Make **ANY** attempt to access the "deep/dark web"; this is an extremely serious violation of the highest nature, that could expose you to illegal, disturbing and malicious content, which may result ~~to~~ in your personal safety being affected. Accessing the Deep Web will also result in the police being involved.
- Store personal files such as videos, photos, documents etc. on the school IT systems
- Reveal or publicise confidential or proprietary information, which includes, but is not limited to:
    - Financial information
    - "Individuals'" Personal information
    - Databases and the information they contain
    - Computer/Network/Other System credentials (such as an individual's Username and Password).

**Printing & Document Disposal Policy**

In order to reduce the waste and potential security violations generated by printing, and to prevent the risk of exposed confidential documentation to unauthorised individuals, Talbot Heath School enforces a Printing & Document Disposal policy as follows:

- Care must be taken so that the individual(s) printing, select Black & White as opposed to Colour to reduce ink wastage unnecessarily.
- Care must be taken to not leave printed confidential material on printers or photocopiers.
- High volume printing should be performed using the photocopiers (e.g. Exam papers), and should **NOT** be printed on Inkjet or Laser printers, unless absolutely necessary.
- Confidential business information and documentation (Including personnel files) must be printed using the secure & confidential options (available on all of the Photocopiers).
- All highly-sensitive/confidential business-related printed matter must be disposed of using confidential waste bins or shredders.
- For large volume printing, users should consult the Reprographics department for advice on how to print in the most cost-effective manner.

**Working Off-site**

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media provided by Talbot Heath School taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried in a protective laptop bag at all times and carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, Smartphones and tablets. They must be protected at least by a password/passcode or a PIN and, where available, encryption.

- Staff that need to create and/or edit highly-sensitive and/or confidential documentation relating to staff personnel and/or students on their personal laptop or home computer are permitted to do so **ONLY** if the file is stored on an encrypted memory stick or encrypted portable media (the IT department will supply you with one). The file **MUST NOT** be saved to your personal computer and stored, sent, copied or distributed.

**Mobile Storage Devices**

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives etc. are permitted for use on the Talbot Heath School IT systems within reason.

However, individuals are **NOT PERMITTED** to store any sensitive and/or confidential information and/or documentation on the media. Should you need to take such information and/or documentation with you (for example) to work on from home, you must contact the IT Department, and ask them to supply you with an encrypted memory stick or other encrypted portable media.

**Individuals must not:**

- Store personal files such as music, video, photographs or games on Talbot Heath School's IT equipment (Including supplied Mobile Storage devices).

**Software**

Individuals must only use software that is authorised and installed by Talbot Heath School on Talbot Heath School's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Talbot Heath School's computers must be approved and installed by the Network Manager for Talbot Heath School's IT department. Individuals are not permitted to try and install software themselves.

**Viruses/Malware**

The IT department has implemented cloud-hosted, Bitdefender Gravityzone which has been installed on every desktop computer, laptop and digital signage device within Talbot Heath School. All of the above systems have the antivirus software installed, to detect and remove any virus proactively, and program and virus definition updates are automatically approved and deployed frequently.

**Individuals must not:**

- Attempt to remove or disable the Anti-Virus Software.
- Attempt to remove virus-infected files or clean up an infection themselves (contact the IT department directly if you suspect or know that a computer or files may be affected by viruses).
- Purposely and with intent, try to place viruses or other malware on **ANY** of the school's IT systems.

**Telephony (Voice) Equipment Conditions of Use**

Use of Talbot Heath School's voice equipment is intended for business use. Individuals must not use Talbot Heath School's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

**Individuals must not:**

- Students are not permitted to use the Mitel desk phones in offices or other locations around the school, unless explicitly permitted to do so by a member of staff.

- Use Talbot Heath School's voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations (or leave voicemails in this manner).
- Accept reverse charge calls from domestic or International operators, unless it is for business use.
- Call outside of the UK, unless explicit permission is given from their head of faculty (Staff) or from a member of staff (Students).

**Mobile Device & Imagery/Video Taking/Recording Conditions of Use**

Use of personal mobile devices by staff is permitted on Talbot Heath School grounds, so long as the individual uses it responsibly, and that Staff members "lead by example". For example, Staff must ensure that their personal mobile device is on silent or switched off when teaching – so as not to cause any disruption(s).
It is also prudent to ensure that the staff users' device is out of sight to avoid any other personnel from seeing something that could be confidential/private.
Users of webcams, cameras, mobile devices (Staff and Sixth Form only) etc. should take extra care that only appropriate images are taken and/or recorded.

**Staff and Students must not:**

- Use mobile devices in lesson hours to make/receive calls, texts, emails, use social media, or play games etc.
- Allow their mobile device to cause a noise disruption in the classroom.
- Students (other than Sixth Formers) are not allowed to use their mobile device for any purpose during the school day. The only exception to this rule is for students who have been given permission by the Lead Nurse and DSL to use their phone for medical purposes, e.g. to check insulin levels. Students with permission to use their mobile device for medical purposes will be given a Yondr medical pouch which is secured by Velcro rather than locked, enabling the student to access their phone when needed.
- Share other individuals' contact telephone numbers with one another without the express permission of the individual first.
- Make hoax or threatening calls to internal or external destinations (or leave voicemails in this manner).
- Take a photo or photos, record sound or video of any individual without getting the individuals explicit permission first. If the photo(s), sound or video is for educational use, this **MUST** be done on the school supplied iPad, and not the individual's personal mobile or other device.
- Use webcams for anything other than educational use – except in the case of boarding students, where they are permitted to use a webcam to contact family.
- Use webcams for any inappropriate use.
- Use webcams with anyone except family and friends that the individual knows in real life.

**Actions upon Termination of Contract**

All Talbot Heath School IT equipment and data, for example laptops and mobile devices including iPads with their chargers and leads, telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Talbot Heath School at termination of contract.

All Talbot Heath School data or intellectual property developed or gained during the period of employment remains the property of Talbot Heath School and must not be retained beyond termination or reused for any other purpose.

**Monitoring and Filtering**

Talbot Heath School exercises its right to monitor the use of computer systems and mobile devices at all times. This will include observing Internet use, examining emails, and deleting inappropriate materials stored on Talbot Heath School ICT systems.
In circumstances where Talbot Heath School believes that unauthorised use of the computer systems is, or may be taking place, or systems are, or may be, being used for unlawful or non-educational purposes, it reserves the right to inform and provide documentary evidence to the appropriate authorities.
**It is your responsibility to report suspected breaches of the ICT Acceptable Usage policy without delay to your line management and to the IT department.**

**All breaches of the ICT Acceptable Usage policy will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Talbot Heath School disciplinary procedures.**