|  |  |
| --- | --- |
| Title | Trelawnyd VA Online Safety Policy |
| Date | April 2023 |
| Author | D Bayliss |
| Approved by head teacher |  |
| Approved by Governing Body |  |
| Next Review Date |  |

**1. Introduction and Overview**

**Rationale**

**The purpose of this policy is to:**

* set out the key principles expected of all members of the school community at Trelawnyd VA with respect to the use of IT-based technologies.
* safeguard and protect the children and staff of Trelawnyd VA.
* assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
* set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
* have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
* ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
* minimise the risk of misplaced or malicious allegations made against adults who work with students.

**The main areas of risk for our school community can be summarised as follows:**

### Content

### exposure to inappropriate content

* content validation: how to check authenticity and accuracy of online content

### Contact

* grooming
* online bullying in all forms

### 

### Conduct

* privacy issues, including disclosure of personal information
* digital footprint and online reputation
* health and well-being (amount of time spent online)
* extremism
* copyright (little care or consideration for intellectual property and ownership – such as music and film)

**Scope**

This policy applies to all members of Trelawnyd VA community (including staff, governors, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school computing systems, both in and out of Trelawnyd VA.

The school 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 Online safety behaviour that take place out of school.

| Role | Key Responsibilities |
| --- | --- |
| Headteacher | * To take overall responsibility for Online Safety provision * To take overall responsibility for data and data security * To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements * To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant * To be aware of procedures to be followed in the event of a serious e-safety incident. |
| Digital leader | * Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents * Promotes an awareness and commitment to Online safeguarding throughout the school community * Ensures that Online safety education is embedded across the curriculum * To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident * Ensures all parents and pupils have signed the Acceptable Use agreement |
| Governors | * To ensure that the school follows all current Online safety advice to keep the children and staff safe * To approve the Online Safety Policy and review the effectiveness of the policy. * To support the school in encouraging parents and the wider community to become engaged in e-safety activities |
| Teachers | * To embedonline safety issues in all aspects of the curriculum and other school activities * To supervise and guide pupils carefully when engaged in learning activities involving online technology * To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws |
| All staff | * To read, understand and help promote the school’s e-safety policies and guidance * To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy * To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies regarding these devices * To report any suspected misuse or problem to the Head Teacher * To maintain an awareness of current online safety issues and guidance. * To model safe, responsible and professional behaviours in their own use of technology * To ensure that any digital communications with pupils and parents should be on a professional level and only through school-based systems. * Only share images online through school approved parent communication apps |
| Pupils | * Read, understand, sign and adhere to the Pupil Acceptable Use Policy * Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations * To understand the importance of reporting abuse, misuse or access to inappropriate materials * To know what action to take if they or someone they know feels worried or vulnerable when using online technology. * To know and understand school policy on the use of mobile phones and handheld devices. * To know and understand school policy on the taking / use of images and on cyber-bullying. * To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home * To help the school in the creation/ review of e-safety policies * To engage with lessons on e-safety and cyber-bullying led by PC McManus |
| Parents/carer | * To support the school in promoting online safety and endorse the Parents’ Acceptable Use Agreement which includes the pupils’ use of the Internet and the school’s use of photographic and video images * To read, understand and promote the school Pupil Acceptable Use Agreement with their children * To consult with the school if they have any concerns about their children’s use of technology * To discuss the safe use of online apps and materials. * To monitor their child's use of online apps and gaming to ensure safe and appropriate use. |

**Communication:**

The policy will be communicated to staff/pupils/community in the following ways:

* Acceptable use agreements discussed with pupils at the start of each year.
* Acceptable use agreements to be issued to whole school community, usually on entry to the school
* Acceptable use agreements to be held in pupil and personnel files
* Made available on the school website.

**Handling complaints:**

* The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
* Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  + informing parents or carers;
  + removal of Internet or computer access for a period,
  + referral to LA / Police.
* Complaints of online bullying and all forms of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

**Review and Monitoring**

* The Online safety policy will be reviewed annually or when any significant changes occur regarding the technologies in use within the school. For example: There is an invitation only Facebook page for parents use and use of the app Seesaw to communicate with parents. An Instagram account has been created to share news and events. Photographs and names of children are not posted on the page. This account is monitored by a member of the SLT. If these are seen to be being misused or as nonsecure then they will be removed from use permanently or until such time as the problem has been addressed.

**2. Education and Curriculum**

**Pupil Online safety curriculum**

Trelawnyd VA

* Has a clear, progressive Online safety education programme as part of the curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
  + to STOP and THINK before they CLICK
  + to NEVER share or save passwords
  + to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  + to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  + to know how to narrow down or refine a search;
  + [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  + to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information including location details private;
  + to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  + to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
  + to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
  + to understand why they must not post pictures or videos of others without their permission;
  + to know not to download any files – such as music files - without permission;
  + to have strategies for dealing with receipt of inappropriate materials;
  + [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;
  + To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
  + To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
* Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas using the DCF as a guide.
* Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
* Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
* Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights;
* Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming / gambling;

**Staff and governor training**

This school

* Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection such as when ctf files are sent school to school via the school secretary;
* Makes regular training available to staff on online safety issues.
* Provides, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school’s Acceptable Use Policies.

**Parent awareness and training**

This school provides guidance for parents, including:

* + Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
  + Information leaflets;

**3. Expected Conduct and Incident management**

**Expected conduct**

In Trelawnyd VA, all users:

* are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
* need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
* 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 online safety practice when using digital technologies out of school and realise that the school’s Online Safety Policy covers their actions out of school, if related to their membership of the school
* will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and online bullying

Staff

* are responsible for reading the school’s Online safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

* should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* should be aware of how to report incidences of cyber bullying and inappropriate use

Parents/Carers

* should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online safety acceptable use agreement form at time of their child’s entry to the school
* should know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse through the agreement signed on school entry.

**Incident Management**

In this school:

* there is strict monitoring and application of the Online safety policy and a differentiated and appropriate range of sanctions
* all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
* support is actively sought from other agencies as needed in dealing with online safety issues
* monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
* parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
* We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

**4. Managing the IT and Computing infrastructure**

* **Internet access, security (virus protection) and filtering**

Trelawnyd VA:

* + Has the educational filtered secure broadband connectivity through the LA which is monitored and kept up to date through the Service Level Agreement
  + All internet activity is logged by the school’s internet provider
  + Uses user-level filtering where relevant, thereby closing or opening options appropriate to the age / stage of the students;
  + Works in partnership with the LA to ensure any concerns about the system are communicated so that systems remain robust and protect students;
  + Is always vigilant in its supervision of pupils’ use, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
  + Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
  + Requires staff to preview websites before use. Plans the curriculum context for Internet use to match pupils’ ability, using child-friendly search engines where more open Internet searching is required.
  + Is vigilant when conducting ‘raw’ image search with pupils e.g. Google image search;
  + Informs all users that Internet use is monitored;
  + Informs staff and students that that they must report any failure of the filtering systems
  + Makes clear all users know and understand what the ‘rules of appropriate use’ are and what sanctions result from misuse – through staff meetings and teaching programme;
  + Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
  + Monitors comments left
  + Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
* **Network management (user access, backup)**

This school

* + Uses individual logins for all adult users;
  + Storage of all data within the school will conform to the UK data protection requirements

*To ensure the network is used safely, this school:*

* Ensures staff read and sign that they have understood the school’s Online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
* Staff access to the schools’ management information system is controlled through a separate password for data security purposes;
* We provide pupils with a class log-in username to access the computer, text code or Qr code to access seesaw, and individual log ins for access to Hwb (which allows them access to Google Classroom if their parents have given permission and email), as well as RM easimaths, Spelling shed and Gigglets.
* Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
* Requires all users to always log off and sign out when they have finished working or are leaving the computer unattended when the computer itself does not lock after a period of idleness;
* Maintains equipment to ensure Health and Safety is followed;
* Has integrated curriculum and administration networks, but access to the Management Information System is set-up to ensure staff users can only access modules related to their role;
* Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
* Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit’s requirements;
* Uses the DfE secure s2s website for all CTF files sent to other schools;
* Follows Flintshire advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
* All computer equipment is installed professionally and meets health and safety standards;
* Reviews the school IT systems regularly regarding health and safety and security.

**Password policy**

* This school makes it clear that staff must always keep their password private, must not share it with others and must not leave it where others can find it;
* When accessing online resources such as Cornerstones hub, Hwb, Assessment foundation, G6 etc. Passwords should not be saved on the browser.
* All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

**E-mail**

**Trelawnyd VA**

* Provides staff with an email account for their **professional** use, and makes clear personal email should be through their own separate account;
* Does not publish personal e-mail addresses of pupils or staff on the school website.
* Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
* Will ensure that email accounts are maintained and up to date
* Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
* Knows that spam, phishing and virus attachments can make e mails dangerous.
* Uses the 2-step verification app to access work emails off site.
* Ensures a healthy work life balance with responding/ reading emails outside of school hours

**Pupils:**

* Pupils’ e-mail accounts are intentionally ‘anonymised’ for their protection.
* Pupils are introduced to and use e-mail as part of the IT/Computing scheme of work.
* Pupils are taught about the online safety and ‘netiquette’ of using e-mail both in school and at home i.e. they are taught:
  + not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  + that an e-mail is a form of publishing where the message should be clear, short and concise;
  + that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  + they must not reveal private details of themselves or others in e‑mail, such as address, telephone number, etc.;
  + to ‘Stop and Think Before They Click’ and not open attachments unless sure the source is safe;
  + that they should think carefully before sending any attachments;
  + embedding adverts is not allowed;
  + that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  + not to respond to malicious or threatening messages;
  + not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  + not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  + that forwarding ‘chain’ e-mail letters is not permitted.
* Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**School website and school social networking**

* + The Headteacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
  + Uploading of information is restricted to our website authorisers
  + The school web site complies with the statutory DfE guidelines for publications;
  + Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status;
  + Photographs published on the web do not have names attached;
  + We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website;
  + We do not use embedded geodata in respect of stored images
  + When using Facebook, Social media accounts, SeeSaw or the Hwb network for school-based tasks appropriate care and diligence should be taken that personal details of pupils, parents and staff are not shared or discussed and that a professional tone is maintained throughout.

**Social networking**

School staff will ensure that in private use:

* No reference should be made in social media to students / pupils, 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.

**5. Data security: Management Information System access and Data transfer**

**Strategic and operational practices**

At this school:

* The Head Teacher is the Senior Information Risk Officer (SIRO).
* We ensure staff know who to report any incidents where data protection may have been compromised.
* All staff are DBS checked and records are held in one central record
* We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system, so we know who has signed.
* staff,
* governors,
* pupils
* parents

This makes clear staffs’ responsibilities regarding data security, passwords and access.

* We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
* We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
* We ask staff to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored. This should be completed ready for the beginning of a new academic year.

**Technical Solutions**

* We require staff to log-out of systems when leaving their computer,
* We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
* All servers are in lockable locations and managed by DBS-checked staff.
* We lock any back-up tapes in a secure, fire-proof cabinet.
* We use an approved disposal company for disposal of equipment where any protected data has been held.
* Paper based sensitive information is shredded.

**6.** **Equipment and Digital Content**

**Personal mobile phones and mobile devices**

* Mobile phones brought into school are entirely at the staff member, students’ & parents’ or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
* Student mobile phones which are brought into school must be turned off (not placed on silent) and given to the class teacher to store. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times.
* The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw authorisation for use at any time if it is to be deemed necessary.
* Police will be called to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
* Where parents or students need to contact each other during the school day, they should do so only through the school’s telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may seek specific permissions to use their phone at other than their break times.
* Staff mobile phones and other personally owned devices will not be used in any way during lessons or formal school time unless specific permission has been given. They should always be switched onto silent.
* Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.

***Students’ use of personal devices***

* **The school strongly advises that student mobile phones should not be brought into school.**
* If a student breaches the school policy, then parents will be contacted, and the matter discussed. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
* If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
* Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

***Staff use of personal devices***

* Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
* Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
* If a member of staff breaches the school policy then disciplinary action may be taken.
* Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

**Digital images and video**

**In this school:**

* We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
* We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
* Staff sign the school’s Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
* If specific pupil photos (not group photos) are used on the school web site or in other high-profile publications the school will obtain individual parental permission for its long-term use
* Pupils are taught about how images can be manipulated in their e-safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work;
* Pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
* Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

**Asset disposal**

All redundant equipment will be disposed of through an authorised agency organised via the service level agreement. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

# Acceptable Use Agreement: Pupils - Primary

**Primary Pupil Acceptable Use Agreement / eSafety Rules**

* I will only use ICT in school for school purposes
* I will only use my class email address when emailing people, I know or people my class teacher has approved.
* I will only open email attachments from people I know, or who my teacher has approved
* I will not tell other people my ICT passwords
* I will only open/delete my own files
* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
* I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
* I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
* I am responsible for my behaviour when using ICT because I know that these rules are to keep me safe
* I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
* I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
* I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
* I will not sign up to online services and social media until I am old enough

Signed: Date:Trelawnyd VA

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.   
  
Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Ms Parsons.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

****

**Parent/ carer signature**

We have discussed this document with ……………………………………..........(child’s name) and we agree to follow the eSafety rules and to support the safe use of ICT at Trelawnyd VA School.

Parent/ Carer Signature …….………………….………………………….

Class …………………………………. Date ………………………………

# 

**Staff, Governor and Visitor**

**Acceptable Use Agreement / Code of Conduct**

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and always adhere to its contents. Any concerns or clarification should be discussed with the Headteacher.

* I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
* I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities or save passwords.
* I will ensure that all electronic communications with pupils and staff are compatible with my professional role
* I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
* I will only use the approved, secure email system(s) for any school business
* I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
* I will not install any hardware or software without permission
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
* Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
* Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
* I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community’
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
* I will respect copyright and intellectual property rights
* I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
* I will support and promote the school’s e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
* I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.
* I understand this forms part of the terms and conditions set out in my contract of employment

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….………………….………… Date ……………………

Full Name …………………………………......................................... (printed)

Job title ……………………………………………………………………