Wood Edge Independent School

Policy covering the use of

ICT equipment and e-Safety guidelines

Incorporating:

Acceptable use of ICT Policy for Users

Review date: October 2024

CONTENTS

Introduction

At Wood Edge Independent School, we are committed to ensuring that our students are able to operate with safety and confidence whenever and wherever they use the Internet or mobile technologies regardless of ability or their additional educational needs.

We understand our responsibility to educate our students in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using technology, in and beyond the context of the classroom.

The school's e-safety policy should operate in conjunction with other policies including those for Safeguarding, Behaviour, Anti- Bullying, ICT Curriculum and Data Protection.

The Internet is an essential element in everyday life, it is part of the statutory curriculum and a necessary tool for staff and students.

The school has a duty to;

- provide students with quality Internet access as part of their learning experience
- provide filtered internet access appropriate to the age of students.
- provide students with clear rules for internet use and how they can keep themselves safe online

Roles and Responsibilities

As e-Safety is an important aspect of leadership within the school, the Head of Education has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The Head of Education will keep up to date on current issues and guidance through appropriate organisations, Lancashire LSCB and the Local Authority.

All staff are responsible for reading and understanding the contents of this policy and the appendices outlining the ICT available to them and how it should be used appropriately. Staff are also responsible for reporting any suspected misuse or e-safety related problems through appropriate monitoring of ICT use. All e-safety related problems are to be reported to the Head of Education.

All students will be taught to understand the importance of e-safety education. Students at Wood Edge School will in most cases, require additional assistance including reminders and prompts of how to remain safe when using the internet. All use of the internet will be well planned and managed to aid the students understanding of internet safety wherever possible.

This Policy will be available to all parents.

Use of ICT Resources including the internet

The internet is an essential element in 21st century life for education, business and social interaction. Our school has a duty to provide students with quality internet access as part of their learning experience.

All other users of ICT at Wood Edge School will be asked to read and understand the contents of this policy and the appendices outlining the ICT available to them and how it should be used appropriately. Their understanding is confirmed through the signing of the ICT 'Acceptable Use Policy' before using any school ICT resource. This applies to staff and external organisations / visitors. The school office will maintain a current record of all individuals who have signed the AUP.

Any e-Safety concerns with regards to the internet must be reported to the Head of Education.

Introducing the e-safety policy to students

An e-Safety education programme will be introduced to raise the awareness and importance of safe and responsible internet use. The school will aim to teach students;

- how to stay safe online
- what is acceptable and what is not acceptable behaviour when using the internet
- not to reveal personal details of themselves or others in any online communication or arrange to meet anyone without specific permission.
- effective use of the Internet in research,
- the skills of knowledge location, retrieval and evaluation
- to be critically aware of the materials they read and how to validate information before accepting its accuracy.

This will be achieved through;

- All students will be supported by their LSA's when using the internet at all times.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained. Staff should recognise the importance of e-safety and demonstrate their acceptance of this policy and their adherence to its contents by signing the Acceptable Use Policy in Appendix 13

The staff will be made aware that this e-safety policy incorporates all intended aspects of their ICT use in school and is explained in Appendix 1 - 12, most notably;

- Online discretion and professional conduct is essential at all times both in and outside of school hours.
- (personal) Mobile phones will not be used during school time.

Staff will be supported through;

- Regular information and training on e-Safety issues in the form of staff meetings
- Access to details of ongoing staff training being displayed in the staffroom
- New staff receive information on the school's acceptable use policy as part of their induction
- Being made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- Encouragement to use the skills learnt to incorporate e-Safety activities and awareness within curriculum areas.

Parents and the e-Safety policy

Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site*. This policy will be placed on the school website*.

*once operational

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

The school cannot accept liability for the material accessed, or any consequences of internet access. This is explained clearly to parents in the information sheet that they are provided.

The school will monitor ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Breaches

All outlined earlier, all staff are responsible for reporting any suspected misuse or e-safety related problems through appropriate monitoring of ICT use. e-safety related problems are reported to the Head of Education.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head of Education.

Additionally, all security breaches, lost/stolen equipment or data, any ICT equipment purchased by the School used by members of staff include: virus notifications, unsolicited emails, misuse or unauthorised use of ICT and use of any 3rd party online storage utility e.g., drop box; Google drive; sky drive, or similar. All other policy non-compliance must be reported to the Head of Education.

The table below indicates sanctions relating to the misuse or misconduct

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the My 3 Limited Disciplinary Procedure. Policy breaches may also lead to criminal or civil Proceedings.

.

Complaints

Complaints of internet misuse will be dealt with by the Head of Education.

- Any complaint about staff misuse must be referred to the Head of Education.
- Complaints of a child protection nature must be dealt with in accordance with the school's child safeguarding procedures.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the schools' behaviour policy.

Reviewing this Policy

This policy will be reviewed annually, and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted.

This policy has been read, amended and approved by the staff, Head of Education and Responsible Individual. There will be an on-going opportunity for staff to discuss with the Head of Education, any issue of e-safety that concerns them.

Antony Maynard

A. Maynard

Head Teacher
October 2023

Appendix 1 - Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The school follows Becta guidelines Becta Schools - Leadership and management - Security - Data handling security guidance for schools (published Spring 2009)

Security

- It is the responsibility of everyone to keep their passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent.

Senior Information Risk Owner (SIRO)

The SIRO in Wood Edge School is the Head of Education who is familiar with information risks and the school's response. Typically, the SIRO should have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

The SIRO in this school is Peter Lam

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, student or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

The handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Appendix 2 - Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through our IT Services provider – Britannia IT Services' collection and disposal service. Any disposal will confirm to WEEE regulations and data protection guidelines.

Appendix 3 - Use of Electronic Mail

The use of e-mail is an essential means of communication for staff. The use of email will be introduced to students as and when it is deemed appropriate and when it is considered that the responsible use of email will be understood by students.

Managing e-Mail

For staff;

- The school gives all teaching and admin staff their own e-mail account. This account should be the only account used for school business
- It is the responsibility of each account holder to keep their password secure.
- Staff must report if they receive an offensive e-mail
- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

For students;

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- The forwarding of chain letters is not permitted in school.
- All student e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Appendix 4 - Internet Access

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

Managing use of the Internet

- Users should not post personal, sensitive, confidential or classified information or disseminate such information about others in any way that may compromise its intended restricted audience
- The school will provide students with supervised access to Internet resources through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use and raw image searches are discouraged when working with students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

Infrastucture

- Wood Edge School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate

- It is the responsibility of the Head of Education to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the Head of Education for a safety check first

- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head of Education.

- If there are any issues related to viruses or anti-virus software, the Head of Education should be informed.

Appendix 5 - Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to students within school
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the school

Appendix 6 - Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to the Head of Education when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- User ID and passwords for staff and students who have left the School are removed from the system within two months

If you think your password may have been compromised or someone else has become aware of your password report this to your Head of Education

Password Security

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

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- Users are provided with an individual email and password
- Students are not allowed to deliberately access on-line materials of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school information, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations/ipads are not left unattended and are locked.

- In our school, all ICT password policies are the responsibility of the Head of Education and all staff and students are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorized access (Microsoft© advise every 42 days)

Further advice available http://www.itgovernance.co.uk/

Appendix 7 - Safe Use of Images

Taking of Images and Film

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

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Consent of Adults Who Work at the School

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

Publishing Student's Images and Work

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas,
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the student attends this school unless there is a change in the student's circumstances where consent could be an issue.

- Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents (where appropriate) in order for it to be deemed valid.
- Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images / films of children should only be stored in the recognised file of the teacher, Head of Education.
- The Head of Education has the responsibility of deleting the images when they are no longer required, or the student has left the school

Webcams and CCTV

- The school may use CCTV for security and safety. This is external in the grounds.

- We do not use publicly accessible webcams in school

Appendix 8 - School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

The school will log ICT equipment issued to staff and record serial numbers as part of the school's inventory. As a user of ICT, you are responsible for

- any activity undertaken on the school's ICT equipment provided to you

- not attempting unauthorised access or unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- personal, confidential or sensitive data stored on the school's network drive or removable media equipment

- returning all ICT equipment and ICT system login details to the Head of Education on termination of employment or resignation.

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your Head of Education immediately.

All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Ensure portable and mobile ICT equipment is made available as necessary for

anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the Head of Education and fully licensed.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Our school chooses to manage the use of these devices in the following ways;

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. These devices should not be used, unless specific permission has been granted by the Head of Education
- Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device unless permission has been sought from the Head of Education
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media you must ensure that;

- The use of recommended encrypted media only
- all removable media is stored securely
- disposal is done in line with this policy

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses.

Appendix 9 - Servers

- Any newly installed servers holding personal data should be encrypted, therefore password protecting data.
- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container
- Back up media stored off-site must be secure

Appendix 10 - Telephone Services

- School telephones are provided specifically for school business purposes, however you may make or receive personal telephone calls provided they are infrequent, brief and are not made for profit or to premium rate services.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- In the event of receiving a telephone call containing a bomb threat. Follow the recognised procedures available from the school office.

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services

You must reimburse the school for the cost of any personal use of your school mobile phone.

Appendix 11 - Social Networking

Online conduct should not be different to offline conduct. Employees using social networking sites in a personal capacity must ensure that they do not;

- Conduct themselves in a way that is detrimental to the School. To do otherwise may lead to formal disciplinary action under the School's Disciplinary Procedure.
- Post offensive, defamatory or inappropriate comments about the School, its students, suppliers or any of its employees.
- Allow interaction on websites to damage or compromise working relationships with colleagues
- Make discriminatory or offensive comments about work colleagues or students.
- Post photographs/videos of themselves, colleagues or students taken in school or which is work related.
- Post or send abusive or defamatory messages
- Record any confidential information about the School on any social networking sites
- Post information which would lead to the identification of a student.
- Accept requests of any student of the School or former students under the age of nineteen to become 'friends' on Facebook or any other social networking site
- It is advisable not to accept requests from the parents or guardians of any student of the School or former students under the age of nineteen to become 'friends' on Facebook or any other social networking site. Should you wish to accept such a request you must seek advice from your Head of Education before doing so.
- Make a request to become 'friends' with any student of the School or former students under the age of nineteen as friends on Facebook or any other social networking site
- Make a request to the parents or guardians of any student of the School or former students under the age of nineteen to become 'friends' on Facebook or any other social networking sites.

This list is neither exclusive nor exhaustive.

Accessing social networking sites during school time must be in accordance with the School's Acceptable Use Policy and breaches may lead to formal disciplinary action.

It may be is necessary to create closed ‘blogs’ and social networking areas for curriculum purposes. Any such activity should be agreed in advance with the Head of Education.

On occasions when it is appropriate for staff and students to share a closed ‘blog’ or social network area for curriculum purposes and permission has been given to do so, appropriate measures must be put in place to ensure the safety of the staff and students.

Appendix 12 – e-safety rules for students

e-safety Rules will be explained to all staff to enable them to deliver the message to children. The e-safety rules will be displayed in each classroom.

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 13 - Acceptable Use Agreement

Student Acceptable Use

- **Agreement / e-safety Rules**

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail 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 deliberately 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 details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

Parent Acceptable Use

Where relevant and depending on their age and ability, your child will be taught the following rules for being **SMART** when using the internet;

Safe – I can remain safe online by not sharing my personal information such as my name, my address or which school I go to.
Meet – I will not arrange to meet anyone in the real world who I have been communicating with using the internet.
Accept – I will think before I click on pop-ups, emails and other messages that may appear on my computer screen.
Reliability – I will consider how much I can trust what I see on the internet, including people who want to be my friend and the information I read on websites.
Tell – If I am worried, upset or not sure what to do, I will tell a member of my family or one of my teachers. I trust them to know what to do.

The school will take every precaution, to ensure that your child remains safe when using the internet. This will be achieved by;

- the provision of quality Internet filtered internet access appropriate to the age of students.
- the provision of clear rules for internet use and how they can keep themselves safe online
- accessing the Internet by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

The school will inform you if it is felt that your child has been exposed to any inappropriate internet content. As a parent or legal guardian, it is assumed that you;

- give permission for your son or daughter to use the Internet whilst attending Newlands Hey.
- understand that due to its changing nature, the school cannot be held responsible for the nature of all material on the internet.
- accept that if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website.
- understand that should an incident occur, you support the school in dealing with this as outlined in the schools e-safety and Behaviour Management policies.
- understand that children' full names will not be used anywhere on the website, particularly in association with photographs

All staff are responsible for reporting any suspected misuse or e-safety related problems to the Head of Education to ensure the online safety of all students.

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, 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 adhere at all times to its contents. Any concerns or clarification should be discussed with Di Jones Head of Education.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head of Education.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that personal data 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 of Education. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Head of Education
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students 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 Head of Education.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- 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 . . . . …