South Farnham Educational Trust
The Continual Pursuit of Excellence

# ONLINE SAFETY POLICY

REVIEW: ANNUALLY LAST REVIEW DATE: AUTUMN 2023

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including the Social Media Policy, Behaviour Policy, Safeguarding Policy and Data Handling Policy.

## Aims

**Great Bookham School aims to:**

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention. to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

South Farnham Educational Trust
The Continual Pursuit of Excellence

## Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## Using this Policy

- The school will form an Online Safety Committee and which will include the Headteacher, Deputy Head and the Computing Co-ordinator.
- The Online Safety Policy has been written based on best practice and government guidance. It has been agreed by Senior Management and approved by Governors.
- The Online Safety Policy was reviewed in Autumn 2023.
- The policy was approved by Trustees in September 2023.
- The Online Safety Policy and its implementation will be reviewed annually. The next review is due in Autumn 2024.
- The Online Safety Policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff or as a pupil.

## Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between our systems and networks and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age-appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.

- Access to school networks will be controlled by **personal passwords.**
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform future Online Safety policies.
- The security of our systems and networks will be reviewed regularly.
- All staff that manage filtering and monitoring systems will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

**All staff's responsibilities for filtering and monitoring:**

- Monitor what is on pupils' screens.
- Teach children about online safety using MTP.
- Know how to report safeguarding and technical concerns, if:
    - You witness or suspect unsuitable material has been accessed
    - You are able to access unsuitable material
    - You are teaching topics that could create unusual activity on the filtering logs
    - There is failure in the software or abuse of the system
    - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - You notice abbreviations or misspellings that allow access to restricted material

**Governors' responsibilities for filtering and monitoring:**

- Make sure the DSL takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role.
- Make sure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of their safeguarding training.
- Review the DfE's filtering and monitoring standards:
- Identify and assign roles and responsibilities
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting T&L
- Have effective monitoring strategies in place that meet their needs
- Discuss with IT staff and service provider what needs to be done to support the school
- Assign a member of SLT and a Governor to be responsible for filtering and monitoring.

**Parents'/Carers' responsibilities for filtering and monitoring:**

- Engage with support and guidance provided by the school to ensure that home devices have appropriate levels of filtering and monitoring in place.
- Monitor their children's online activity, including mobile phone use, to ensure that they are behaving responsibly and appropriately online.
- Notify the school with any concerns or incidents relating to inappropriate activity online.

South Farnham Educational Trust
The Continual Pursuit of Excellence

**Educating Pupils About Online Safety - Curriculum**

Great Bookham School will provide an age-appropriate Online Safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety (including age restrictions, content and personal data).

Pupils will be taught about Online Safety as part of the curriculum based on the National Curriculum for Computing. It is also taken from the guidance on relationships education, relationships and sex education and health education (RSHE).

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

**Educating Parents and Carers about Online Safety**

We will endeavour to raise parents/carers' awareness of online safety in letters or other communications home, as well as providing up-to-date information via the dedicated Online Safety page on our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will inform parents/carers of:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or a member of the Online Safety Committee.

## Protocols

**Email**

- Staff may only use approved email accounts on our systems and networks.
- Incoming email should be treated as suspicious and attachments should not be opened unless the author is known.
- Pupils will be given restricted email accounts in line with safeguarding procedures.

**Published Content – e.g. School Website, school social media accounts**

- The contact details will be the school address, email and telephone number. Staff and pupil's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing pupils' images and work**

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in the Surrey Safeguarding Children Board Guidance on using images of children.

**Use of social media including the school learning platform**

- The school has a separate social media policy.
- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Use of video services such as Zoom will be monitored by staff and will be limited to class based activities.
- Staff and pupils should ensure that their online activity both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the community.

**Use of personal devices**

- Personal equipment may be used by staff to access our systems and networks provided their use complies with the Online Safety Policy and the Acceptable Use Policy.
- Staff must not store images of pupils or pupil personal data on personal devices.

- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

**Protecting personal data**

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to school systems.

## Policy Decisions

**Authorising Access**

- All staff (including teaching staff, teaching assistants, support staff, office staff, trainee teachers, work experience trainees, ICT technicians and governors) must read and sign the Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy before accessing our systems and networks.
- The school will maintain a current record of all staff and pupils who are granted access to our systems and networks.
    - **At Key Stage1**, access to the internet will be by adult demonstration with supervised access to specific, approved online material, which supports the learning outcomes planned for the pupils age and ability.
    - **At Key Stage 2**, access to the internet will be with teacher permission and supervision but with increasing levels of autonomy, using age-appropriate search engines and online tools.
- People not employed by the school must read and sign an Acceptable Use of Computers, IT Equipment, Internet and Email (Visitors) Policy before being given access to the internet via school equipment.
- Parents/carers will be asked to sign and return a consent form (Acceptable Use of the School Computers) to allow use of technology by their child.

**Assessing risks**

- 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. Neither the school nor SFET can accept liability of the material accessed or any consequences of internet access.

## Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

## Harms and Risks

### Navigating the Internet and Managing Information

- Pupils will learn how to navigate the internet safely as part of their Computing lessons (details can be found in the Computing Policy).
- Due to the complex nature of the internet, pupils will be encouraged to consider information presented to them with caution, ensuring that they consider the reliability of the source.
- Topics will include considering age restrictions, disinformation/misinformation, fake websites and scam emails, online fraud and personal data (including protecting passwords and privacy settings)

### Staying Safe Online

- Alongside the Computing curriculum content, pupils will learn how to stay safe online from outside agencies, including the Police and the NSPCC.
- Pupils will receive age specific advice covering the following topics:
    - online abuse (e.g. sexual harassment, bullying, trolling and intimidation)
    - online challenges and identifying whether they are safe or not
    - content which incites
    - fake profiles (i.e. adults posing as children or 'bots')
    - grooming (e.g. radicalisation, Child Sexual Abuse and Exploitation and gangs)
    - risks linked to live streaming
    - interacting with known contacts to avoid unsafe communication

### Wellbeing

- At Great Bookham School, we ensure that pupil's wellbeing is continually monitored through discreet PSHE lessons, including Relationships Education, and opportunities where pupils can voice their concerns.
- As part of this learning, pupils will look specifically at online safety relating to screen time use and allowances, and how people's behaviour can differ online and offline.
- These lessons will be conducted in a safe and trusting manner, where pupils will be encouraged to follow the 'SMART' guidance for staying safe online.

## Communication of the Policy

### To Pupils

- Pupils need to agree to comply with the pupil Acceptable Use of School Computers Policy in order to gain access to our systems and networks and to the internet.
- Pupils will be reminded of the contents of the Acceptable Use of School Computers Policy as part of their Online Safety education.

**To Staff**

- All staff will be shown where to access the Online Safety Policy and its importance will be explained.
- All staff must sign and agree to comply with the Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy in order to gain access to the school's systems and networks and to the internet.

**To Parents**

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website.
- Parents will be offered Online Safety training annually.

## Mobile Technology Guidance

**Staff and Visitors use of personal devices**

- Mobile phones and personally-owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Mobile phones and personally-owned 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 devices.
- No images or videos should be taken on mobile phones or personally-owned devices, including on school trips or out of school activity – only school provided equipment will be used for this purpose.
- Staff are not permitted to use their mobile phones or personal devices for contacting pupils, young people or those connected with the family of a student.
- If a member of staff breaches the school's policy, then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to the lunchbreak and after school.

**Pupil use of mobile devices**

- Parents wishing for their child to bring a mobile phone into school must notify the school and give their permission in advance. Pupils must then hand their device into the office on arrival. No mobile phones or personal devices including Smart watches are to be kept in classrooms or cloakrooms during school hours – the only exception being those requiring their mobile phone to monitor medical support systems such as Dexcom diabetes monitoring systems.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use the school phone, in the school office. Parents are asked not to contact their child via their mobile phone during school hours but to contact the school office.
- Pupils should protect their mobile phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices.

- If a pupil breaches the school's policy, then the phone or device will be confiscated and it will be held in a secure place in the school office. Mobile phones and devices will be released to parents and carers in accordance with school policy.

## Vulnerable Children

- Any pupil can be vulnerable online and their vulnerability is affected by their age, developmental stage and personal circumstance.
- Great Bookham School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Great Bookham School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum, Great Bookham School will seek input from specialist staff as appropriate, including the SENCO.

## Useful Links for Educational Settings

### National Organisations for Schools

- The Anti-Bullying Alliance: www.anti-bullyingalliance.org.uk
- Childnet: www.childnet.com
- DotCom Digital: https://dotcomdigital.co.uk/
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation: www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- UK Safer Internet Centre: www.saferinternet.org.uk
    - 360 Degree Safe: www.360safe.org.uk

### National Organisations for Parents/Carers

- Internet Matters: www.internetmatters.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parent Info (CEOP and Parent Zone): https://parentinfo.org
- Parent Zone: https://parentzone.org.uk/parents

### National Organisations for Pupils

- BBC Own It: https://www.bbc.com/ownit includes links to their Own It app.
- Childline: www.childline.org.uk

## Appendices

**Appendix 1**: Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy and Agreement

**Appendix 2**: Pupil and Parent/Carer Acceptable Use of School Computers Agreement

**Appendix 3**: Acceptable Use of Computers, IT Equipment, Internet and Email (Visitor) Policy and Agreement

South Farnham Educational Trust
The Continual Pursuit of Excellence

# Responsible Use of Computers, ICT Equipment, Internet and Email (Staff)

**The Computer Network (including laptops and other ICT peripherals) is owned by the school. This statement helps to protect staff by clearly stating what use of computer resources is acceptable and what is not. The use of any part of the Computer Network without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.**

1. All network access must be made via the user's authorised account and password, which must not be given to any other person.

2. All users accounts can and will be monitored as directed by the Head Teacher.

3. School computer use and Internet use must be appropriate to staff professional activity. Where laptops have been provided, they may be used outside the school's premises for professional activities only. Laptops are not covered by the school's insurance when they are off school property. They must not be left unattended at anytime, both on and off school premises.

4. School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share
- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally
- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment
- to collect, store or send personal information about children or adults without direct reference to The Data Protection Act/GDPR
- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project
- to use the school's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or Computing Coordinator if applicable.

5. Copyright and intellectual property rights must be respected.

6. The use of personal email accounts within school is strictly prohibited. Certain members of staff are provided with a school email account which can be used for communication with third party as directed by the Head Teacher.

7. All email accounts are monitored by the Head Teacher, supported by the ICT Technician. Emails should be written carefully and politely and authorised before sending, in the same way as a letter written on school headed paper.

8. The forwarding of chain letters via email is not permitted.

9. In accordance with the procurement procedures of the school, individuals must not order items via the Internet or by email. Any orders must be processed by the designated office staff.

10. The use of Internet Chat rooms, Instant messaging services and Internet Notice Boards is strictly prohibited unless authorised for professional activity by the Head Teacher. Microsoft Teams is an exception.

11. The use of portable media such as floppy disks, memory sticks and CD-ROMs is not allowed without permission from the Head Teacher or Computing Coordinator.

12. Downloading applications or software from the Internet or from CD-ROMs is not allowed without permission from the Head Teacher or Computing Coordinator.

13. Computers, particularly laptops, will be regularly serviced by the ICT Technician. Please tell the Computing Coordinator or ICT Technician immediately if you have concerns about a machine.

14. Staff should consider carefully if they need a hardcopy of a document before they print, especially if they are printing a large, coloured document.

15. Children must not use the Internet or the school's email unsupervised at any time. If a teacher wishes pupils to use the Internet or email, this must take place in a room where a member of staff is present at all times.

16. Peripherals are kept in the ICT Technician's office which is out of bounds to all staff except: the Head Teacher, the ICT Technician, the Computing Coordinator and other individuals granted permission by the Head Teacher.

17. Digital cameras and digital videos may only be used for school activities. Care must be taken when taking photographs of children which may only be used within the school. If photographs are required for external presentations, the Head Teacher must be consulted before they are used. After using the digital cameras/videos, any photographs should be stored appropriately on the system and the SD card cleared before returning the camera to its storage location.

18. Personal cameras, including Smartphones are not permitted for the usage of photographing children.

19. Smartphones are not permitted to be used for the sending or receiving of school related data and information, unless the device has been provided by the Academy Trust.

*20.* Take care around all ICT equipment, always follow safety advice and report any breakages or problems, however minor they may seem, immediately to the Computing Coordinator or ICT Technician.

---

**Declaration of Understanding:**

I confirm that I have read and understood the **Responsible Use of Computers, ICT Equipment, Internet and Email (Staff) policy.** I understand that the school may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of email and the saving and retrieval of files contained in the Network User areas and on laptops. I accept receipt of the laptop below on the understanding it is for professional use only and the school has the right to request the return with immediate effect wherever it sees fit.

**Signed……**
**Name in Print……**
**Laptop Number……**
**Date……**

South Farnham Educational Trust
The Continual Pursuit of Excellence

# Acceptable Use of the School Computers

## Pupil and Parent Agreements

Dear Parent/Carer,

All pupils at Great Bookham School will use the computer facilities, including the Internet, as part of their learning and as required by the National Curriculum. The school takes every reasonable precaution to keep pupils safe and to prevent them from accessing inappropriate materials.

These steps include:

- a filtering system
- a monitoring system
- vigilant oversight of all pupils' computer files and Internet access
- the teaching of Online Safety
- the requirement that pupils and parents/carers observe Online Safety rules

Computing provides an exciting and challenging learning opportunity for the children that embraces the technology and methodology which is such an important part of our world.

We would like both pupils and parents/carers to sign the agreements to show that the Online Safety rules have been read and understood.

Please would you be so kind as to read, sign and return the agreements attached to the school office.

Yours Sincerely

Miss J Allen
Headteacher

South Farnham Educational Trust
The Continual Pursuit of Excellence

# Acceptable Use of the School Computers

## Pupil Agreement

As a pupil of Great Bookham School :

1. I will take care of the school computers.
2. I will not give my username and/or password or any personal information to anyone.
3. I will only use the Internet when I have been given permission by an adult.
4. I will only use websites provided by a teacher or a teaching assistant.
5. I will tell an adult if I see anything that makes me uncomfortable, worried or unsure.
6. I will always be polite and friendly when I write messages on the internet.

.....

**My Name: .....**

**Date: .....**

**Please complete, sign and return to the school office**

South Farnham Educational Trust
The Continual Pursuit of Excellence

# Acceptable Use of the School Computers

## Parent/Carer Agreement

As a Parent/Carer of a pupil at Great Bookham School:

1. I have discussed the Pupil Agreement with my child to ensure their understanding.
2. I accept that, ultimately, the school cannot be held responsible for the nature and the content of materials accessed through the internet but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
3. I understand that the school is not liable for any damages arising from my child's use of the internet facilities.
4. I will support the school by promoting safe use of the Internet and digital technology at home and I will inform the school if I have any concerns over my child's Online Safety.
5. I will not distribute any photographic images of children on social media networks or using any other photographic format.

.....

**Name (Printed): .....**

**Parent /Carer Signature: .....**

**Date: .....**

**Please complete, sign and return to the school office**

South Farnham Educational Trust
The Continual Pursuit of Excellence

# Acceptable Use of Computers, IT Equipment, Internet and Email (Visitor)

1. I understand that I have been given use of the school internet and/or the school's systems and networks in order to carry out a specific job for the school.
2. I understand that it is a criminal offence to use the systems and networks for a purpose not permitted by its owner.
3. I will use the school's systems and networks for the purpose for which I have been given access.
4. I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
5. I will not install software without the permission of the Headteacher and Computing Coordinator.
6. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school's systems and networks.
7. I understand that all my use of the internet and other related technologies can be monitored and logged and it can be made available, on request, to the Headteacher or my employer.
8. I will respect copyright and intellectual property rights.
9. I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

.....

**Declaration of Understanding:**

I confirm that I have read and understood the **Acceptable Use of Computers, IT Equipment, Internet and Email (Visitor) policy**. I understand that the school may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of email and the saving and retrieval of files contained in the Network User areas and on laptops.

**Full Name: ..... (Printed) Company: .....**

**Signed: ..... Date: .....**