



# Walter Infant School

## E-Safety Policy

### DOCUMENT HISTORY

Version	Action	By	Date
1.1	Draft	Rob Waller	Oct. 2011
1.2	Re-draft	Rob Waller	Jan 2012
1.3	Re-draft	Rob Waller	April 2012
1.4	Re-draft	Rob Waller	Jan 2013
1.5	Approved	Full Governing Body	25 March 2013
1.6	Re-draft	David Turner	Feb 2014
1.6	Approved	Full Governing Body	March 2014

**Next Review Date:**

**Under Review by Policy and Review  
Committee – 2016**

# Walter Infant School

## E-Safety Policy

### 1 E-Safety Policy Introduction

- 1.1 E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration and publishing tools. It highlights the need to educate pupils and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- 1.2 This e-Safety Policy:
  - 1.2.1 Replaces the previous Staff Internet and Email Policy and the Internet Access Policy for Children which have been revised and renamed as the school's E-Safety Policy. This reflects the need to raise awareness of the potential personal and commercial safety issues associated with electronic communications as a whole. It aims to ensure that all employees understand their responsibilities and the School's expectations of the manner in which these systems are used.
  - 1.2.2 Will operate in conjunction with other school policies including those for ICT, Behaviour, Safeguarding, Curriculum Planning and Health & Safety.
  - 1.2.3 Applies to all employees and other workers within the school, whether full or part-time, as well as agency workers, temporary workers and contractors. The policy does not form part of member of staff's terms and conditions of employment and may be amended from time to time.
  - 1.2.4 This E-Safety policy has been written by the school, and is strongly influenced by a template provided by Wokingham Borough Council which itself is based on the work of the Kent County Council E-Safety team, Radstock Primary School and the "360° Safe" School e-Safety Self- Review Toolkit . This E-Safety Policy and its implementation will be reviewed annually.
- 1.3 Further information can be found at:  
[wsh.wokingham.gov.uk](http://wsh.wokingham.gov.uk) <http://www.swgfl.org.uk/safe>  
<http://www.nen.gov.uk/esafety>
- 1.4 In setting and monitoring this policy, the School will comply with the individual rights of employees and any legislative requirements.
- 1.5 Useful Information and contacts  
SWGfL Staying Safe – <http://www.swgfl.org.uk/Staying-Safe>  
Childnet International – <http://www.childnet-int.org/>  
CEOP – <http://www.thinkuknow.co.uk>  
The Byron Review – <http://www.dcsf.gov.uk/byronreview/>

## 2. ICT Teaching and Learning

Please refer to the Walter Infant School ICT Policy.

## 3. Roles and Responsibilities

### 3.1 Governors

Governors are responsible for the approval of the e-Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In fulfilling this responsibility the governing body may appoint an ICT governor. Governors will require/undertake the following regular activities:

- Meetings with the ICT Co-ordinator.
- Monitoring of e-safety incident logs.
- Keeping up to date with school e-safety matters.

### 3.2 Headteacher

The Headteacher is responsible for ensuring the safety, including e-safety, of members of the school community. The day to day responsibility for e-safety may be delegated to the ICT Co-ordinator or another appropriate member of staff. However, the Headteacher will ensure the following:

- Staff with e-safety responsibilities receive suitable and regular training enabling them to carry out their e-safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular updates.
- There is a clear procedure to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The registration with the Information Commissioner's Office is maintained and the school is kept abreast of regulatory requirements and recommendations as outlined on their website at [www.ico.gov.uk](http://www.ico.gov.uk). SLT should be informed where school policies may require updating.

[See 'Appendix 1 – School and the Data Protection Act' for further information]

### 3.3 ICT Co-ordinator

The ICT Co-ordinator has day to day responsibility for e-safety issues and takes a leading role in establishing and reviewing the school e-Safety Policy and associated documents. The e-Safety Co-ordinator will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide materials and advice for integrating e-safety within schemes of work and check that e-safety is taught on a regular basis.
- Liaise with the local authority on e-safety matters.
- Liaise with the school's technical staff on e-safety matters.
- Ensure that e-safety incidents are reported and logged and used to inform future e-safety developments.
- Report to and meet with the ICT governor and SLT as required.

The ICT governor should be trained in e-safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming

- Cyberbullying

### **3.4 ICT Technician**

The ICT Technician will, in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- The ICT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the e-safety technical requirements outlined in any relevant local authority e-safety policy/guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy.
- The school's filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- E-safety technical information is kept up to date, applied as necessary and passed on to others where relevant.
- Use of the network and learning platform is monitored and any misuse/attempted misuse reported to the ICT Co-ordinator or designated person for investigation and action.
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media.

### **3.5 Teaching and Support Staff**

Teaching and support staff are responsible for ensuring that:

- They are familiar with current e-safety matters and the school e-Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the ICT Co-ordinator for investigation and action.
- Digital communications with pupils (messages/learning platform/voice) should be on a professional level and only carried out using approved school systems.
- Pupils understand and follow Walter's Web Code.
- Pupils have a good understanding of e-Safety in relation to their age.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and implement school policies with regard to these devices.
- They are aware of the procedure for dealing with any unsuitable material that is found during internet searches.

## **4, Reviewing, Reporting and Sanctions**

### **4.1 Review**

4.1.1 This policy will be reviewed and updated annually, or sooner if necessary.

4.1.2 The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective on a yearly basis.

### **4.2 Acceptable Use Agreements**

4.2.1 All users of the school computers will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils (See Appendix 4 )

- 4.2.2 Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.

### 4.3 Course of Action

- 4.3.1 If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific):

**The user should:**

- Turn off the monitor or minimise the window.
- Report the incident to the teacher or responsible adult.

**The teacher/responsible adult should:**

- Ensure the well-being of the pupil.
- Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
- Report the details of the incident to the ICT Co-ordinator.

**The ICT Co-ordinator will then:**

- Log the incident and take any appropriate action.
- Where necessary report the incident to the Internet Service Provider (SEgfl) so that additional actions can be taken.

### 4.4 Complaints regarding internet use

- 4.4.1 Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- 4.4.2 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- 4.4.3 If any member of staff have grounds to believe they have been subjected to behaviour which is discriminatory or harassing as a result of another employee's use of the ICT systems, a complaint should be made under the School's Equal Opportunities Policy.

### 4.5 Sanctions

- 4.5.1 Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- 4.5.2 All staff should also be aware that the downloading and distribution of pornography can constitute a criminal offence. If in the course of a disciplinary investigation it is found that such an offence has been committed, the School reserves the right to report such behaviour to the police.
- 4.5.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

## 5. Communications & Communication Technologies

### 5.1 Mobile phones and personal handheld devices

- 5.1.1 Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
- 5.1.2 Pupils will not be allowed to bring in mobile devices, such as iPods and those which allow ad hoc networks to be established.
- 5.1.3 Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.

- 5.1.4 Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- 5.1.5 Staff, helper and visitor mobile devices may normally be switched off or on silent during the times that children are present.
- 5.1.6 No device in the school should contain content that is inappropriate or illegal.
- 5.1.7 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

## 5.2 E-mail and messaging

- 5.2.1 Staff will be informed that use of school e-mail or messaging accounts will be monitored.
- 5.2.2 Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- 5.2.3 Access by pupils to external e-mail accounts whilst in school will not be permitted. Any email communication will be carried out by staff members.
- 5.2.4 Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- 5.2.5 Pupils may only use approved internal message accounts on the school system.
- 5.2.6 Pupils should not reveal details of themselves or others, such as address or telephone number.
- 5.2.7 Information of a sensitive nature should not be sent by e-mail.
- 5.2.8 The forwarding of chain letters will not be permitted.

## 5.3 Social networking

- 5.3.1 For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, blogs, chat rooms, online gaming, YouTube, Instant Messenger, etc.
- 5.3.2 By default the SEgfl will block/filter access to external social networking sites.
- 5.3.3 Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for infant aged pupils.
- 5.3.4 Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- 5.3.5 Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- 5.3.6 The use of internal social networking tools, e.g. blogs, wikis, messaging, etc., within a school learning platform is both acceptable and to be encouraged.  
[See '*Appendix 3 – Social Networking Guidance*' for further information]

## 5.4 Internet usage

- 5.4.1 The school Internet access is designed expressly for pupil use and includes filtering by South East Grid for Learning ("SEgfl") appropriate to the infant age of pupils.
- 5.4.2 The school will work with Wokingham Borough Council and SEgfl to ensure systems to protect pupils are reviewed and improved.
- 5.4.3 If staff or pupils discover an unsuitable site, it must be reported to the Internet Service Provider via the ICT Co-ordinator.
- 5.4.4 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- 5.4.5 Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- 5.4.6 Pupils will be taught what Internet use is acceptable and what is not.

- 5.4.7 Pupils will be educated in the effective use of the Internet in research (including the skills of knowledge location, retrieval and evaluation) using the internally hosted Espresso service.
- 5.4.8 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- 5.4.9 The school will keep a record of all pupils who are granted access to the Internet/Learning Platform. This record will be kept up-to-date. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- 5.4.10 Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- 5.4.11 Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- 5.4.12 All pupils using the internet, and associated communication technologies, will be made aware of the school's e-Safety Guidelines. These should be posted near to the computer systems.
- 5.4.13 Pupils will receive guidance in responsible and safe use on a regular basis
- 5.4.14 Parents will be asked to sign and return a consent form and discuss the Walters Web Code with their children before being given a login to the learning platform. Walters Web Code will be published prominently on the school website at: [www.walter.wokingham.sch.uk](http://www.walter.wokingham.sch.uk)

## 5.5 Digital and video images

- 5.5.1 Parents, staff and pupils may record images of pupils at school under the following conditions:
- 5.5.2 All staff digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- 5.5.3 Images should not be distributed beyond either the school or the immediate family and friends of the pupil's family.
- 5.5.4 Images should not be posted on an open internet site, e.g. on a social networking page with the permissions set to public or on the school learning platform and/or website on an open page.
- 5.5.5 On the public side of the learning platform and/or website, photographs may only show unclear pictures of pupils so that no individual child can be identified.
- 5.5.6 Pupils' full names may not be used on the learning platform and/or website in conjunction with photographs or video.
- 5.5.7 No images of pupils should be recorded
  - in toilets or wash areas
  - whilst pupils are getting changed
  - in the medical room
- 5.5.8 The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g. how to wash hands). In this case the line manager must be informed before this activity is undertaken.
- 5.5.9 The use of staff devices is not acceptable unless agreed with a member of SLT in advance.
- 5.5.10 Images of pupils must be stored securely and deleted when no longer required.

## 5.6 Learning platform and/or website

- 5.6.1 The school learning platform and/or website should include the school address, school e-mail, telephone and fax number including any emergency contact details.



- 5.6.2 The school learning platform and/or website should be used to provide information and guidance to parents concerning e-safety policies and practice.
- 5.6.3 Staff or pupils' home information should not be published.
- 5.6.4 The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.
- 5.6.5 Pupil's work will only be published on the Learning Platform (for school access only) with the permission of the pupil and parents.

## **6. Infrastructure and Security**

### **6.1 Security**

- 6.1.1 The school in conjunction with SEgfl will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.
- 6.1.2 School ICT technical staff may monitor and record the activity of users on the school ICT systems and users will be made aware of this.
- 6.1.3 Servers, and communications cabinets should be securely located and physical access restricted.
- 6.1.4 Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- 6.1.5 All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician.
- 6.1.6 Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- 6.1.7 The 'Administrator' passwords for the school ICT system, used by the ICT Technician are also available to the ICT Subject Leader and must be stored securely in school.
- 6.1.8 School ICT systems, capacity and security will be reviewed regularly.
- 6.1.9 Internet searches will not be carried out in a classroom environment by pupils. In classroom environments staff will only use safe search engines such as Espresso or Purple Mash.

### **6.2 Passwords**

- 6.2.1 All staff are provided with an individual password. The pupils use a year group login. All users will have an individual log on to the learning platform and/or secure areas of the website.
- 6.2.2 No individual should tell another individual their password.
- 6.2.3 No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil for monitoring/testing purposes.
- 6.2.4 Once a computer has been used, users must remember to log off so that others cannot access their information.
- 6.2.5 The school enforces a password change policy .passwords are changed every three months.
- 6.2.6 In the event that a password becomes insecure then it should be changed immediately.

### **6.3 Filtering**

- 6.3.1 The school maintains and supports the managed filtering service provided by South East Grid for Learning (SEGfL).
- 6.3.2 Changes to network filtering should be approved by the ICT Subject Leader and the ICT Technician.



6.3.3 Any filtering issues should be reported immediately to SEGfL.

## **6.4 Virus protection**

- 6.4.1 All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
- 6.4.2 The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only dependable sources should be used.
- 6.4.3 Staff should have access to and be able to use security software to remove adware and malware.

## **6.5 Staff laptops/devices**

- 6.5.1 The following security measures should be taken with staff laptop/devices:
  - Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
  - Laptops/devices should never be left in a parked car, even in the boot.
  - Screen savers should be set to lock after a maximum of 15 minutes.
  - Laptops/devices should not normally be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.

## **6.6 Personal and sensitive data**

- 6.6.1 All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- 6.6.2 Sensitive data is any data which links a child's name to a particular item of information and:
  - must be encrypted on laptops/devices, memory sticks, CDs and other removable media;
  - should not be e-mailed between staff;
  - should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
- 6.6.3 Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.
- 6.6.4 There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.
- 6.6.5 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

[See '*Appendix 3 – Sensitive and Non-Sensitive Data*' for further information]

## **6.7 Loading/installing software**

- 6.7.1 For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.
- 6.7.2 Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- 6.7.3 Only authorised persons, such as the ICT Technician/Network Manager or ICT Subject Leader, may load software onto the school system or individual computers.

- 6.7.5 Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

## **6.8 Backup and disaster recovery**

- 6.8.1 The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:
- The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
  - No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
  - Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
  - Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.
- 6.8.2 The school should have a whole school ICT disaster recovery plan which would take effect when severe disturbance to the schools ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised.

## **7. E-Safety Education**

### **7.1 Learning and teaching for pupils**

- 7.1.1 Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- 7.1.2 Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- 7.1.3 Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- 7.1.4 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- 7.1.5 Key e-safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- 7.1.6 E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

### **7.2 Staff training**

- 7.2.1 All staff will be given the School e-Safety Policy and its importance will be explained.
- 7.2.2 Staff will be kept up to date through regular e-safety training.
- 7.2.3 Staff should always act as good role models in their use of ICT, the internet and mobile devices.

### **7.3 Parental support**

- 7.3.1 Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site. The support of, and partnership with, parents should be encouraged. This is likely to include the following:
- Awareness of the school's policies regarding e-safety and internet use; and where appropriate being asked to sign to indicate agreement.
  - Practical demonstrations and training.

- Advice and guidance on areas such as:
  - filtering systems
  - educational and leisure activities
  - suggestions for safe internet use at home

## Appendix 1 – School and the Data Protection Act

1. The Seventh Principle of the Data Protection Act (1998) states that:  
*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
2. This means that schools must have appropriate security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.
3. The implications of this for the school will be the need to:
  - Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
  - Be clear about who is responsible for ensuring information security.
  - Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
  - Respond to any breach of security swiftly and effectively.
4. Failure to comply with the Act could result in loss of reputation or even legal proceedings.
5. Further guidance may be found at [www.ICO.gov.uk](http://www.ICO.gov.uk)

## Appendix 2 – Social networking guidelines

### 1. Staff conduct

- 1.1 Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- 1.2 Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' online space.

### 2. Access to social networking sites

- 2.1 Social networking sites should not be used or accessed during school working hours.
- 2.2 Staff may not use school equipment to access social networking sites.
- 2.3 If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

### 3. Posting of images and/or video clips

- 3.1 Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
- 3.2 Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

### 4. Privacy

- 4.1 Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- 4.2 Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- 4.3 Staff should not create new links with parents simply because they teach their children.
- 4.4 Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- 4.5 Any changes to social networking sites and privacy settings should be clearly understood.

### 5. Additional considerations

- 5.1 Thought should be given to what the implications of this policy will be for the different groupings within the staff employed at the school, e.g.
  - Teacher
  - Teaching assistant
  - Other support staff, e.g. bursar, site manager, lunchtime supervisors, office staff, cleaners
- 5.2 Outside agency staff, e.g. sports coaches, music tutors, etc.





## Appendix 3 – Sensitive & Non-sensitive data

1. Sensitive data will include:
  - SEN records such as IEPs and Annual Review records
  - Mark sheets and assessments
  - Reports and Open Evening comments
  - Personal data stored on the school's Management Information System, e.g. SIMS
  - Photographic or video material
  - Name, address and contact information
2. Non-sensitive data thus includes:
  - General teaching plans
  - Curriculum materials
  - General correspondence of a non-personal nature

## **Appendix 4 – Acceptable Use Agreements**

1. The following are acceptable use agreements referred to within this policy.
2. The use agreements included are:
  - Laptop Acceptable Use Agreement
  - Staff Code of Conduct
  - Pupil Code of Conduct: Walter's Web Code

## Laptop/Devices Acceptable Use Agreement

### 1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's e-Safety Policy
- All recipients and users of these devices should read and sign the agreement.

### 2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

### 3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

### 4. Faults

- In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

### Declaration:

I have read and understood the above and also the school's e-Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

## Staff Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

1. I understand that it may be viewed as a criminal offence to use a school ICT system for a purpose not permitted by its owner.
2. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
3. I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
4. I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
5. I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
6. I will not install any software or hardware unless authorised, e.g. on a school laptop.
7. I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school e-Safety policy.
8. I will respect copyright and intellectual property rights.
9. I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
10. I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
11. I will ensure that pupil use of the internet is consistent with the school's e-Safety Policy.
12. When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
13. I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
14. I know what to do if offensive or inappropriate materials are found on screen or printer.
15. I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. e-Safety Co-ordinator and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	










## Pupil Code of Conduct: Walter's Web Code

# Walter's Web Code

Walter Infant School and Nursery

Guidelines for the Use of the Learning Platform

To keep safe when I am using the learning platform and the internet:

-  I will always ask an adult before I use a computer.
-  I will only search the web if an adult is with me to help.
-  I will only use websites that my school and my parents say are safe.
-  I will only log on with my own username and password and I will not use one that belongs to someone else.
-  I will not tell anyone else my learning platform password and I will always log off from the platform when I have finished.
-  I know that images and text on the web belong to somebody else and I should not copy them and use them on the learning platform.
-  I will be sensible about what I put on the learning platform.
-  I know that I shouldn't send unkind messages to anyone.
-  I will tell an adult if I find anything that upsets me on the internet.

I know that I can only use the platform if I agree with all these rules.