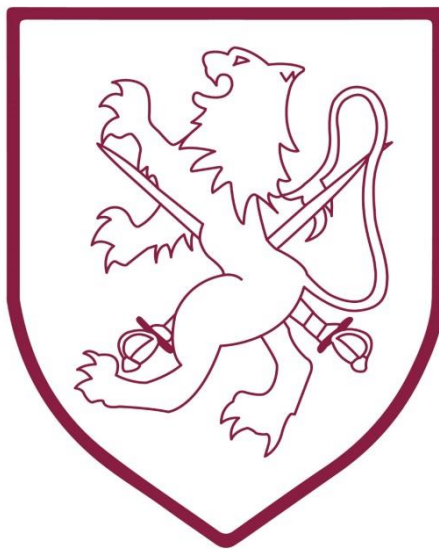




**WOKINGHAM  
BOROUGH COUNCIL**



# **Walter Infant School and Nursery**

## **E-Safety - All in one Model Policy**

### **DOCUMENT HISTORY**

<b>Version</b>	<b>Action</b>	<b>By</b>	<b>Date</b>
1.1	Approved	Full Governing Body	November 21 <sup>st</sup> 2017
1.2	Awaiting Approval	Full Governing Body	Spring Term 2020

**Review Date: Biannually – Spring 2022**

# 1 Roles and Responsibilities

## 1.1 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 choose to appoint an e-safety governor and establish an e-safety committee with appropriate representation.

Governors will require/undertake the following regular activities:

- Meetings with the e-Safety Co-ordinator/Computing Leader.
- Monitoring of e-safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school e-safety matters.

## 1.2 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 e-Safety Co-ordinator, Computing Subject Leader 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 monitoring reports.
- There is a clear procedure to be followed in the event of a serious e-safety allegation being made against a member of staff.

## 1.3 E-Safety Co-ordinator/Computing Leader

The e-Safety 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.
- Liaise with the school's technical staff.
- Ensure that e-safety incidents are reported and logged and used to inform future e-safety developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

## 1.4 Technical Support

The School Administration Team and the Computing Leader, in co-operation with the school's technical support provider, will 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, in which passwords are regularly changed.
- 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, learning platform and pupil e-mail is regularly monitored and any misuse/attempted misuse reported to the e-Safety 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.
- Provide secure access to the school network from home where necessary using VPN or equivalent technologies.

## 1.5 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 e-Safety Co-ordinator for investigation and action.
- Digital communications with pupils (e-mail/learning platform/voice) should be on a professional level and only carried out using approved school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's e-Safety and Acceptable Use Policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations 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 that they monitor their use and implement school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

## 1.6 The Designated Safeguarding Leaders

The DSLs 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

## 1.7 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping 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]

## 2 Reviewing, Reporting and Sanctions

### 2.1 Review

- This policy will be reviewed and updated annually, or sooner if necessary.
- The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

### 2.2 Acceptable Use Agreements

- All users of the school computers will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.
- All users will be expected to resign agreements on a regular basis.  
[See 'Appendix 6 – Exemplar Acceptable Use Agreements' for further information]

### 2.3 Reporting

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.  
[See 'Appendix 2 – Course of action if inappropriate content is found' for further information]

### 2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

### 2.5 Sanctions

- 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.
- 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.

## 3 Communications & Communication Technologies

### 3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
  - Where mobile phones are allowed in school they may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images is forbidden.
  - Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
  - 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.
  - Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
-

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

### 3.2 E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored.
- Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils may only use approved e-mail or message accounts on the school system.
- Pupils should immediately tell a staff member if they receive an offensive e-mail or message.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Pupils wishing to send e-mails to an external person or organisation must be authorised by a member of staff before sending.
- Information of a sensitive nature should not be sent by unencrypted e-mail.

### 3.3 Social networking

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, Skype, Second Life, etc.

- 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.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- The use of 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]

### 3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- 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.
- 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.
- Unauthorised users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- 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.
- Pupils will receive guidance in responsible and safe use on a regular basis

### 3.5 Digital and video images

Although it is recognised that there will be some variation in the approach taken by different schools to the taking and use of digital and video images of pupils, the majority of points noted below should feature in most school policies. Where the school chooses to vary from the guidelines they should have clearly thought through the reasons for doing so, made this clear in their policy, ensured consistency with other policies such as Safeguarding, and informed all those concerned.

#### Parental permission

- The school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use could include the school website, learning platform or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- If specific individual pupil photographs are to be used publicly, such as on the school website, in the prospectus or any other high profile publication, then a check should be made with individual parents for this additional use.
- Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

#### Storage and deletion

- All images of pupils will be securely stored in one central location.
  - Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin.
  - Images of pupils should normally be deleted once a pupil has left the school unless being kept as part of archived records. Such retention, and the period involved, should be specified in the Data Protection or Data Retention policy.
-

### **Recording of images**

- All staff and pupils must sign the ICT Acceptable Use Agreement.
- School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online 'cloud' storage) care must be taken that the location of images of pupils is clearly understood and in line with ICO (Information Commission's Office) guidance.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.

### **Use of staff personal devices**

It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. Where a school wishes to vary from this, e.g. for off-site activities, the following should apply:

- It will be clearly understood under what circumstances it is permissible to use a personal device.
- Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies deleted.
- Such staff personal devices should be passcode protected.

### **Parents taking photographs or video**

Where the school chooses to allow the recording of images at 'public' events the following should apply:

- Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

### **Events/Activities involving multiple schools**

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.



### 3.6 Learning platform and/or website

- The school learning platform and/or website should include the school address, school e-mail, telephone and fax number including any emergency contact details.
- The school learning platform and/or website should be used to provide information and guidance to parents concerning e-safety policies and practice.
- Staff or pupils' home information should not be published.
- 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.

## 4 Infrastructure and Security

### 4.1 Security

The school 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.

- 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.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- 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/Network Manager.
- 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.
- The 'Administrator' passwords for the school ICT system, used by the ICT Technician/Network Manager are also available to the ICT Subject Leader and must be stored securely in school.

### 4.2 Passwords

All staff are provided with an individual password. Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the learning platform and/or secure areas of the website.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- Once a computer has been used, users must remember to log off so that others cannot access their information.
- Users leaving a computer temporarily should lock the screen (Windows key + L).
- Passwords should be changed at regular intervals. The school may choose to enforce this requirement through the use of Windows Password Policy where passwords are changed for example every three months.
- In the event that a password becomes insecure then it should be changed immediately.

[See 'Appendix 4 – Password guidance' for further information]

### 4.3 Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

---



- Changes to network filtering should be approved by the ICT Subject Leader and the ICT Technician/Network Manager.
- Any filtering issues should be reported immediately to the ISP and/or SEGfL.

#### 4.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
- 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.
- Staff should have access to and be able to use security software to remove adware and malware.

#### 4.5 Staff laptops/devices and flash drives

Staff laptops/devices and flash drives are likely to be taken out of school and may well contain sensitive data (see Section 3.6). Schools should encrypt staff laptops and staff should only use school provided encrypted flash drives.

The following security measures should also 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.
- Screensavers should be set to lock after a maximum of 15 minutes.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

[See 'Appendix 6 – Exemplar Acceptable Use Agreements' for further information]

#### 4.6 Personal and sensitive data

- 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.
- Sensitive data is any data which links a pupil's name to a particular item of information and/or the loss of which is liable to cause individuals damage and distress. Therefore, such data:
  - must be encrypted on laptops/devices and any 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.
- 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.
- 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.

[See 'Appendix 5 – Sensitive & Non-Sensitive Data' for further information]

#### **4.7 Electronic devices - search and deletion**

Schools now have the power to search pupils for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices. Clear guidelines relating to this should be communicated to staff and parents. Such guidelines will include:

- Details of which items are banned under the school rules and may be searched for
- A list of staff members/roles authorised to examine and/or erase data on electronic devices
- Clear guidance as to what is, and is not, allowed when searching a pupil
- When data will be deleted or kept as evidence
- How incidents will be recorded

#### **4.8 Loading/installing software**

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the ICT Technician/Network Manager or ICT Subject Leader, may load software onto the school system or individual computers.
- 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.

#### **4.9 Backup and disaster recovery**

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.

The school should also define 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, including who would be involved in this process and how it would be accomplished.

---

## **5 E-Safety Education**

### **5.1 Learning and teaching for pupils**

- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key e-safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers should be displayed in all rooms and displayed next to fixed site computers.

### **5.2 Staff training**

- Staff will be kept up to date through regular e-safety training.
- Staff should always act as good role models in their use of ICT, the internet and mobile devices.

### **5.3 Parental support**

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

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.*

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.

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.

Failure to comply with the Act could result in loss of reputation or even legal proceedings.

Further guidance may be found at [www.ico.gov.uk](http://www.ico.gov.uk)

---

## **Appendix 2 – Course of action if inappropriate content is found**

- 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 e-Safety Co-ordinator.
- The e-Safety Co-ordinator will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

## **Appendix 3 – Social networking guidelines**

Specific guidelines relating to staff use of social networking are best arrived at through discussion to both clarify and agree exactly what should be applicable. Aspects will also be applicable to those associated with the school, e.g. governors and parent helpers.

The following areas should be included in any policy:

### **Staff conduct**

- 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.
- 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.

### **Access to social networking sites**

- Social networking sites should never be accessed during timetabled lessons and other contact with pupils and not normally during school working hours.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

### **Posting of images and/or video clips**

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

### **Privacy**

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

### **Additional considerations**

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
  - Outside agency staff, e.g. sports coaches, music tutors, etc.
-

## Appendix 4 – Password guidance

This guidance is intended for those adults using school systems but is based on good practice and should also feature in the teaching of, and advice to, pupils.

- Passwords should have a 'strength' of at least 12 where a letter is 1 and a number or punctuation mark is 2. The choice of password 'strength' should be appropriate to the data being protected and the potential risks associated with that data being compromised.
- Passwords should avoid following a pattern or being predictable.
- Passwords must not be easily guessable by anyone and therefore should not include:
  - Names of family, friends, relations, pets etc.
  - Addresses or postcodes of same
  - Birthdays
  - Telephone numbers
  - Car registration numbers
  - Unadulterated whole words
- Try to use in a password:
  - A mixture of letters and numbers
  - Punctuation marks
  - At least 8 digits



## **Appendix 5 – Sensitive & Non-sensitive data**

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

Non-sensitive data thus includes:

- General teaching plans
  - Curriculum materials
  - General correspondence of a non-personal nature
-

## **Appendix 6 – Exemplar Acceptable Use Agreements**

The following are included as possible starting points in developing appropriate agreements and guidelines for individual schools. It is highly unlikely that they will be suitable without amendment and are also likely to require consultation with the respective stakeholders.

The exemplars included are:

- Exemplar Laptop Acceptable Use Agreement
- Staff Acceptable Use Agreement
- Parent/Carer and Pupil Acceptable Use Agreement

## **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 Acceptable Use Agreement

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.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- 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.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- 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.
- I will respect copyright and intellectual property rights.
- 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.
- 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.
- I will ensure that pupil use of the internet is consistent with the school's e-Safety Policy.
- 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.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- 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:	

## Internet Use for Children (Parental Approval)

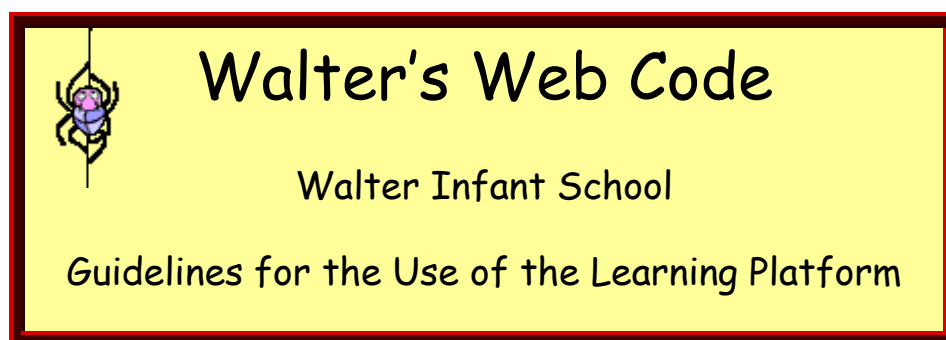
At Walter Infant School IT is an important part of a pupil's education and its use is integrated throughout the school curriculum. As part of their IT learning experience, the school has a duty to provide pupils with quality internet access.

The school has an E-Safety Policy which sets out the school's policy for staff and pupils on IT use and is available to view on the School website. We also ask parents to discuss Walter's Web Code with their child – see below.

Please sign below to give consent for your child to access the internet during school under supervision from staff.

I agree for my child to access the internet during school lessons

Signed ..... Date .....



**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 of these rules**

I understand and agree to abide by the guidelines for use of the school learning platform

Child's signature: .....

Parent's signature: ..... Date: .....

---