E Safety and Data Protection Policy

Contents

1. **Rationale**
2. **Internet Use: Education**
3. **Internet Use: Pupil Access**
4. **Internet Use: Expectations of Pupils**
5. **Internet Use: Expectations of Adults**
6. **Website Guidelines**
7. **Email Guidelines**
8. **General Security and Data Protection Guidelines**
9. **Social Media (Twitter)**
10. **Staff Code of Conduct**

1. Rationale

At Webster Primary School we believe that the benefits of technology and internet access far outweigh the disadvantages. It is our responsibility as educators to ensure that our pupils can use such technologies effectively although, ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using media and information resources is one that school staff share with parents and carers.

Teachers will use carefully selected material from the internet to support teaching and learning in line with curriculum policies. However, by its nature, on occasions, the use of the internet will provide access to information that has not been viewed by a member of staff. Measures are in place to ensure that children do not access unsuitable and inappropriate material online. We use a combination of site-filtering and supervision and aim to foster a responsible attitude to internet use by our pupils in partnership with parents/carers. We present assemblies on the theme of e-safety annually.

Parents and children are required to read and sign an e-safety agreement on admission. This is renewed at the beginning of each academic year. This includes options to allow children to access the internet in school and to have their photograph and/or work included in the school website.

All members of staff are required to sign an e-safety agreement. Any visiting teachers or personnel who wish to use our ICT and internet facilities will be required to sign an agreement to our e-safety rules.

The purpose of this policy is to:

- Establish clear ground rules for school internet use.
- Describe how these fit into the wider school context.
- Demonstrate methods used to protect children from sites containing inappropriate and extreme material.
- Describe school's approach to data protection in general.

2. Internet Use: Education

The benefits of using the internet for education are:

- Access to a wide variety of educational resources.
- Rapid and cost effective worldwide communication.
- Better understanding of global diversity.
- Professional development for staff.
- Exchange of curriculum and administration data with LA and DfE.
- Reward/leisure use.
- Cross curricular application of IT skills.

We teach pupils about the vast information resources available on the internet and use it as a planned part of many lessons.

All staff will review and evaluate resources available on the internet appropriate to the age range and ability of the pupils being taught and the Co0mputing subject leader will assist in the dissemination of this information.

Depending on their age, pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using a specific group of websites. These will be preloaded for children in Foundation Stage and KS1, with children being taught the discrete skills of independent and safe use in order to learn how to access material in KS2.

As part of the Computing curriculum children will be taught how to use search engines and how to safely send and receive email. Children may only use approved search engines which will limit the chances of them being exposed to unsuitable material.

3. Internet Use: Pupil Access

Webster Primary School only uses Computeam's 'filtered' internet service, which minimizes the chance of pupils encountering undesirable material. Filters are updated weekly by our support provider Computeam. Unsuitable sites are blocked as they become known.

We only allow children to use the internet when there is a responsible adult present to supervise. Members of staff will be vigilant in guarding against potential misuse and will be responsible for explaining to pupils the expectations that we have of them and for sharing the e-safety rules which differ between age phases.

4. Internet Use: Expectations of Pupils

- All pupils are expected to read and sign the e-safety agreement and to abide by our e-safety rules.
- Pupils must ask permission before accessing the internet and have a clear reason for doing so.
- We expect all pupils to share our high expectations for behaviour while using the internet, just as they are held responsible for their behaviour in all aspects of school life. This includes the material that they access and the language that they use.
- Pupils using the worldwide web are only to access sites which have been selected for them and are expected to report immediately to teachers any offensive material which they encounter. The only exceptions to this are when pupils are being taught how to conduct an internet search, during which they will be closely supervised.
- Computers should only be used for homework, school work and leisure use which is agreed as a reward in line with school behaviour systems.
- For copyright and security reasons, no computer programmes should be brought from home.

- The internet should never be used to disclose personal information or to make arrangements to meet people.

5. Internet Use: Expectations of Adults

- All teaching and administrative staff are expected to read and sign the adult e-safety agreement and to abide by our e-safety rules.
- Adults are responsible for their own behaviour on the internet and should act as positive role models for all Webster pupils.
- Adults may use the internet to source teaching materials.
- Adults with school laptops may download teaching material to their laptop which is directly relevant to planning and teaching.
- Teachers should only use their encrypted school Portable Drives to store and transport planning and teaching documents for use in school.
- Permission must be granted from the School Business Manager or Computing subject leader for adults to download software onto school computers.
- Applications can only be downloaded onto school iPads by the School Business Manager.
- Adults may access email in school that is related to their daily work.
- Only school cameras/iPads should be used for photographing school pupils and school work. Permission to use any other camera device must be obtained from the Principal/Head of School.
- All images of children should be downloaded then deleted from cameras/iPads and stored safely as soon as possible after the photographs have been taken.

6. Website Guidelines

Our school website is a valuable resource and children's contributions are valued highly. The site will be used to celebrate good work, promote the school, publish information, store resources for projects and homework and provide links to other good sites of interest. Images of children are used as a means of celebrating achievement, encouraging and motivating.
We use the website to actively promote e-safety. This agenda features on the homepage and has its own 'pencil' and section of the site.

- Photographs will only be used with parents'/carers' permission.
- We only publish children's first names on our website, and never have photos and names together.
- Only the school's point of contact will be published on the site. No personal email addresses will be disclosed.
- Any children's work published on the site will reflect the high standards that are expected from all pupils across the school.

7. Email Guidelines

- All messages sent via the school's email system, even personal emails, are considered the intellectual property of Webster Primary School. Privacy cannot be guaranteed in anything that is created, stored, sent or received on the school's email system. Emails can be monitored without prior notification if the school deems this necessary.
- Where there is evidence that guidelines set out in the policy are not being adhered to, the school has the right to take disciplinary action.

- The system will automatically report any emails that contain inappropriate information. It is strictly prohibited to:-
  - send or receive emails containing libellous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature it should be forwarded to the administrator account (admin@webster.manchester.sch.uk) where it will be dealt with.
  - send inappropriate email messages or chain mail. If you receive such messages these should be forwarded to the administrator account.
  - forge or attempt to forge email messages, or disguise or attempt to disguise your identity whilst sending an email.
  - send copyrighted material or forward a message or attachment belonging to another without the permission of the originator first.
  - open suspicious or unrecognised emails or attachments that may put the school system at risk. If in doubt, always speak to the Computing Subject Leader, School Business Manager, Principal, Head of School or Computeam technician.
- Users must take the same care in drafting an email as they would for any communication. What is said in an email can, even unwittingly, constitute a legally binding and enforceable contract. Particular care should be taken in expressing personal opinions on school emails, not least where such views could be interpreted as being the school's opinion, thus leaving the school liable.
- It is understood that emails can be written in an informal style.
- Confidential information can be sent via email, but with care.
- Copies of all emails are saved for a period of two weeks automatically by the system, in the user's personal sent box unless this setting has been changed by the user.
- Although Webster's email system is meant primarily for school use, school does allow the system to be used for personal use as long as it does not interfere with work and users adhere to the email policy.

8. General Security and Data Protection Guidelines

- General security of all school hardware and networks: All our systems are protected by ***ESET Nod 32 Antivirus*** software (Professional Version). This is recommended by our technical support team as the market leading software. It updates itself on a regular basis, often daily.
- Administration network: the administration network is backed up remotely every 24 hours.
- Passwords: all members of staff are issued with a school email address to which they allocate a password. All SIMS users also have a personal password. All staff laptops/P.C.'s and office P.C.'s/iPads are password protected and set to enter stand-by mode if unattended. All passwords are used on a *need to know* basis. Copies of all passwords are kept in the school safe.
- Use of Portable Drives: relevant staff members are provided with encrypted Portable Drives. No other drives should be used on the school premises. It is the individual staff member's responsibility to ensure data is backed up and protected in case of loss or theft.
- **Data considered to be sensitive or personal must not be stored on teacher laptops**. At Webster Primary School we define personal/sensitive data as follows (using guidance from the Information Commissioner's Office).
  - any data from which an individual can be identified. This may not always be a name. (E.g. a combination of age, gender and address could make someone identifiable.
  - particular information about individuals, for example concerning educational attainment levels, family background, racial or ethnic origins, religious beliefs, physical or mental health.

- any data which informs or influences actions or decisions affecting and identifiable individual.

- For the purposes of ensuring accurate teaching plans and assessments, children's initials (only) will be used on relevant documents. This provides an extra layer of protection in addition to encryption. These documents are never stored on teacher laptops, and are only transferred on our securely encrypted Portable Hard Drives.
- **Any documents saved on** Portable Drives**, even though encrypted, (e.g. lesson plans/assessments) should contain pupils' initials only.** The only permitted exceptions to this are Special Needs or Child Protection documentation and statutory documents such as end of year reports which need to have greater detail (full names) in order to ensure accuracy of identification when passed between agencies.
- Social networking: all social networking sites except Twitter are blocked.

9. Statement on Use of Social Media (Twitter)

Purpose for Usage

We believe that social media are an essential 21st century tool for learning, communication, networking and business. In our school we see 'twitter' as the best social media tool to use in order to enhance teaching and learning, communication with parents and marketing of the school. We agree with the following Ofsted guidance that it is our role to support children and families to understand and manage online risk safely:

- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school.

In order to keep everyone as safe as possible while online, we observe the following guidelines.

Guidelines

1. The school account tweets items of professional or promotional interest to parents, teachers, extended family members, governors and community partners.
2. We are fully aware of the potential for inappropriate or offensive material to be posted on twitter by others. Our page/feed is managed by the Principal and member of staff in charge of the Website. We recognise that the account must be well managed and check it on a **daily** basis.
3. Teachers may set up accounts of their own or for their class, using generic names only such as @Year6Webster or @Miss_Smith, in order to tweet news of events in class or school. Teachers must make the school account manager aware of these accounts by 'following' @WebsterPrimary. No such account should exist without being 'followed' by the school account.
4. Only members of school staff have the authority to post tweets. Where they wish pupils to tweet from a class account (e.g. news, a blog or opinion), this is strictly controlled by the teacher, and account passwords are kept securely.
5. Members of staff never use the private messaging function within twitter. All messages must be on the public function.
6. The school account manager may retweet items of interest from these accounts on the main school account.

7. **All tweets posted on any Webster account are in the public domain and must be representative of the aims and ethos of the school and the rationale outlined in the Introduction above.**
8. Although the nominated age for twitter is 13, we are aware that some of our parents allow their children to have an account. Although the 'follow' list of the school account is checked regularly, this remains the responsibility of the parent/carer.
9. This policy links directly to our e-safety policy and all agreements re publishing of children's images are adhered to, notably that no images are posted without parental permission and pupil names are never posted with photos.
10. Staff members may have private personal accounts. If they become aware that pupils are 'following' them, they should block immediately. No tweets with links to personal addresses will be retweeted by school.

Computing

Staff Code of Conduct

Computing and related technologies such as email, internet and the use of mobile devices are an expected part of our daily working life. This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT. This agreement should be read alongside our E-Safety and Data Protection Policy. All members of staff are expected to sign and adhere to its contents.

Internet

- Adults are responsible for their own behaviour on the internet and should be a positive role model for pupils.
- Adults can use the internet to research and augment teaching and learning activities and source materials for use with pupils.
- Adult use of the internet can be monitored and made available to the Principal, Head of School and Governors. Adults will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Email

- Adults will only use school email addresses for any school business.
- Use of personal email accounts is permitted for non-school business during non-contact time providing it does not interfere with work and complies with our Email Guidelines.
- Adults never share personal email addresses with pupils.

Mobile Phones

- Adults will only use personal mobile phones during breaks, lunchtime or PPA and will keep them on silent mode during lessons except in an emergency situation with the agreement of their line manager.
- Adults will not use mobile phones to photograph or video pupils.

Laptops and iPads

All staff must undertake reasonable precautions to protect their laptop and any data stored on it. Specifically:

- The laptop/iPad is not to be left in a car at any time. This includes a locked boot. The school's insurance does not cover equipment stolen from cars.
- It is strongly recommended that the laptop/iPad is not left on the front or back seats of a car whilst in transit.
- If you are travelling by public transport keep the laptop/iPad close at all times.
- If the laptop/iPad is accidentally damaged in any way, the School Business Manager is to be informed immediately.
- Management of data is subject to the provisions of the Data Protection Act and the Freedom of Information Act.

- The laptop/iPad is for your use only, on official school business. Personal use is permitted on the understanding that this usage is fully compliant with school's e-Safety policy.
- There is no requirement for you to insure the laptop/iPad, but you should consider informing your home contents insurer that you have this equipment at home.
- You should not store any data on this laptop/iPad in case of loss or theft leading to sensitive or confidential data being stolen. Please only use your encrypted Portable Drive provided by the school to store any data going off-site.
- The laptop/iPad can be checked on a termly basis by a representative of school's IT provider.
- Adults undertake to return/iPad the laptop on termination of employment by the school, or when a reasonable request is made by the school to do so at any time.

Cameras

- Only school photographic devices should be used for photographing pupils and school work. Permission of the Principal/Head of School must be sought to use a personal camera for school events.
- All images of children should be downloaded as quickly as possible and deleted permanently from the photographic device.

Flash (Pen)Drives/Memory Sticks/Portable Hard Drives

- Only Portable Drives encrypted with appropriate software should be used. These are available from the School Business Manager.
- The Portable Drive remains the property of Webster Primary School. It has been placed in your care and is your responsibility; any loss or damage must be paid for.
- Adults will take all reasonable steps to ensure that Portable Drives are fully virus protected.
- All data going off-site *must only* be stored and transported on this Portable Drive.
- Even though encrypted, any data saved on the Portable Drive should contain children's initials only.
- It is your responsibility to ensure that all data is backed up and any sensitive data is encrypted.
- Whilst employed by Webster Primary School all work and data that you create remains the intellectual property of Webster Primary School. If you leave Webster Primary School, the Portable Drive must be returned with all data on it.

Use of Social Media

- Adults will abide by school's Social Media Policy and ensure that their online activity, both in school and outside school, will not bring their professional role into disrepute.

General

- No hardware or software should be installed or downloaded without the permission of the Computing Subject Leader or School Business Manager.
- Adults are expected to promote e-Safety and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand that this code of conduct forms part of the terms and conditions set out in my contract of employment. I agree to follow this Code of Conduct and to support the safe use of Computing and ICT throughout the school.

Name……..……..Signature..... Date.....