

Witherley C.E. Primary School



E-Safety Policy

Reviewed: Summer 2023
Next review: Summer 2024

Witherley CE Primary School - E-safety Policy

Introduction

Witherley CE Primary School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at Witherley CE Primary School want to ensure that new technologies are used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give disabled pupils increased access to the curriculum to enhance their learning.

We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

The nominated senior person for the implementation of the School's e-safety policy is the Headteacher.

Scope of Policy

The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

Witherley CE Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;
- close supervision of pupils when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

Partnership working

Wetherley CE Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the empsn who provide a managed (not 'locked down') network system. We fully support and will continue to work with empsn to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures.

We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

Use of internet, mobile & digital technologies

We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

Wetherley CE Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:¹ These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users are not allowed to:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs

¹ For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Software piracy
- Other criminal activity

In addition, users are not allowed to:

- Use the empsn or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves empsn or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of empsn or member Local Authorities or adversely impact on the image of empsn;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of empsn, or to empsn itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via empsn
- Undertake activities with any of the following characteristics:
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the empsn network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after empsn has requested that use cease because it is causing disruption to the correct functioning of empsn;
 - other misuse of the empsn network, such as introduction of viruses.
- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Reporting Abuse

There may be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident immediately.

The School also recognises that there may be occasions where pupils may be the victims of inappropriate behaviour that could lead to possible or actual significant harm. This should always be reported to the headteacher in a timely manner. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures² assist and provide information and advice in support of child protection enquiries and criminal investigations.

Education and Training

Wetherley CE Primary School recognises that digital technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use internet & digital technologies safely.

To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.
- Equip school staff with the knowledge and expertise to support pupils in the safe and appropriate use of internet, mobile & digital technologies.
- Work with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our policies and procedures.

Monitoring

Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use.

With regard to monitoring trends, within the school and individual use by school staff and pupils, Wetherley CE Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

Currently, the school is using the industry-standard and school-appropriate Securus software to monitor all internet use on the school system. All inappropriate internet use can be identified and connected with a single, identifiable user. Evidence of misuse is recorded to legal standards and may form part of a subsequent police investigation.

We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our

² Chapters 5, 9, 12 and 13 of the LSCB Procedures

pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

Pupils should not bring mobile phones into school unless requested for use after school e.g. a child walks home alone from school. In these circumstances mobile phones are kept in the school office until home time.

Sanctions

We will support pupils and staff as necessary in the event of a policy breach.

Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

- *Child / Young Person*
 - The child/young person will be disciplined according to the behaviour policy of the school.
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
- *Adult (Staff and Volunteers)*
 - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

If inappropriate material is accessed, users are required to immediately report this to the Headteacher so this can be taken into account for monitoring purposes.