Policy:	**E-Safety Policy** **(non statutory)**	
This policy was adopted or reviewed on:	**October 2018**	
Review Date:	**October 2020**	

Signed_____ (Chair of Governors) Date _____

Contents

1. Introduction

1. Scope of Policy

3. Infrastructure and Technology
   - 3.1 Partnership working

4. Policies and Procedures
   - 4.1 Use of new technologies
   - 4.2 Reporting abuse

5. Education and Training

6. Standards and Inspection
   - 6.1 Monitoring
   - 6.2 Sanctions

7. Working in partnership with Parents and Carers

8. Appendices of the E-safety Policy

Appendix A: Be Skilled Data Collection Sheet

Appendix B: Authorised Acceptable Use Policy – Staff, Volunteers and Governors

1. Introduction

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

1.2 As part of our commitment to learning and achievement we at Oxley 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.

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

1.4 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.

1.5 The nominated senior person for the implementation of the School's e-Safety policy is **Jason Gilman, Headteacher**.

1.6 Linked policies and documentation. This policy supports and links with:

- Child Protection and Safeguarding Policy
- Data Protection (GDPR) Policy
- Teaching and Learning Policy
- Business Continuity Plan
- School Inventory

2. Scope of Policy

2.1 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.

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

- a list of authorised persons who have various responsibilities for E-safety;
- 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.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Oxley Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is **Lightspeed Systems** who provide a managed (not 'locked down') network system. Locally, this system is managed by **Shepshed High School**, within the **Shepshed Learning** secure network. We fully support and will continue to work with to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 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.

3.1.3 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.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

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

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

<u>Users are not allowed to:</u>

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.

4.1.3 The school recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.4 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
- Software piracy
- Other criminal activity

4.1.5 <u>In addition, users are not allowed to:</u>

- Use the school broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves the broadband provider or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of Schools Broadband or member Local Authorities or adversely impact on the image of Schools Broadband;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of embc, or to embc 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 Schools Broadband.
- Undertake activities with any of the following characteristics:
- wasting staff effort or networked resources, including time on end systems accessible via the embc network and the effort of staff involved in support of those systems;

- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- using the embc 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 embc has requested that use cease because it is causing disruption to the correct functioning of embc;
- other misuse of the embc 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.

4.1.6 Where Schools Broadband / Lightspeed Systems become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

4.2.1 There will 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 be report the incident immediately.

4.2.2 The school also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances LSCB[2] Procedures should be followed. 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 Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

5.1 Oxley Primary School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

5.2 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 new technologies safely.

5.3 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.

- Monitor the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely 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 e-safety policies and procedures .

6. Standards and Inspection

We recognise the need regularly review policies and procedures in order to ensure that our practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 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. Lightspeed Systems sends the school a weekly report of suspicious activities, detailing any attempts to access unathorised sites, whether or not access was blocked and which device was being used at the time.

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, we will audit the use of the Internet and email 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.

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

6.2 Sanctions

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

6.2.2 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.

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

7. Working in Partnership with Parents and Carers

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 Related aspects of the school's E-safety policy include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention.

---

[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.
[2] Chapter 9 of the LSCB Procedures
[3] Chapters 5, 9, 12 and 13 of the LSCB Procedures

Appendix A

Be Skilled data collection sheet

Please complete the information below and return to the school office **by Friday XX September.**

SURNAME:		LEGAL SURNAME:	
FORENAME:		MIDDLE NAMES(S):	
CHOSEN NAME:		GENDER:	
DATE OF BIRTH:		YEAR GROUP:	
ADDRESS:			
POSTCODE:		CLASS:	
EMAIL FOR NEWSLETTERS & COMMUNICATIONS		TELEPHONE:	

Please give details of all persons who have parental responsibility(PR) and anyone else you wish to be contacted in an emergency.**Please ensure for any third party information you provide (emergency contacts) that you have their permission to share their personal information with us.** Please record them in the order you wish for them to be contacted.

	PR? Y/N	NAME	RELATIONSHIP	CONTACT DETAILS	
				ADDRESS(if different from above)	HOME/MOBILE/WORK
1					
2					
3					

MEDICAL INFORMATION

DOCTOR:	
SURGERY ADDRESS:	
PHONE NUMBER:	
MEDICAL INFORMATION:	

ADDITIONAL INFORMATION:

DIETARY NEEDS:		RELIGION:	
ETHNICITY:		HOME LANGUAGE:	

The school is registered under the Data Protection Act for holding personal data. The school has a duty to protect this information and keep it up to date. The school is required to share some of this data with the Local Authority and DFE.

SIGNATURE:_____

DATE:_____

(Parent/Guardian with legal responsibility for the child named)

PARENT/GUARDIAN PERMISSION & AGREEMENT FORM

Please tick against each statement and sign to acknowledge you have read and agree to the following:

- ❑ I give permission for my child to be taken out of school grounds for educational visits within the local neighbourhood.
- ❑ I give permission for my child to take part in sporting events which may or may not include travelling by coach.
- ❑ I give permission for my child to eat food, which is a product of cooking, or food tasting sessions within the school curriculum. Please give details of any foods that must be avoided:

  _____
- ❑ I understand that my child is not allowed to wear earrings (ear studs only) during the school day for Health & Safety reasons.
- ❑ I grant permission for my daughter or son to have access to use the internet, e-mail and other ICT facilities at school, under supervision, as part of lessons. **Please note:** the school has strong filtering and firewall systems to prevent inappropriate material being accessed by pupils. For more details, please read our e-safety policy on the school website or you can request a paper copy from the office.
- ❑ I agree to the school using photographs and video of my child. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school (newsletters, school website), and for no other purpose.
- ❑ I agree to the sharing of information about my child with other relevant agencies (eg.health/social services)
- ❑ I give permission for my child to watch films with a PG rating.
- ❑ In the event of an emergency do you give consent to:

Anaesthetics Yes/No
Blood transfusion Yes/No
Appropriate medical intervention Yes/No

_____

Please read the following advice issued by Leicestershire Education Authority:

"Parents and relatives of pupils should note that any photography or video film they take at school events are likely to contain images of other children whose parents will not have given permission for them to be filmed or photographed. Such images should not be circulated more widely than the family, i.e. they should just be for the family's use. Our advice is that any manipulation or distribution of images of children could result in prosecution."

SIGNATURE:_____ (Parent/Guardian with legal responsibility for the child named) DATE:_____

Appendix B

Acceptable Use Policy and Staff agreement form

This policy and agreement covers the use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to unauthorised users.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- **I will not take part in social networking sites with current pupils or those who are under 18 years of age.**
- I will only use the approved school email; school VLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will take precautions when using data transfer devices such as memory sticks eg only using them to transfer data from computers with up to date defence systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided to support my professional responsibilities.
- I will ensure any confidential data is protected by password
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- **I will obtain written permission from the Headteacher** before I connect any personally owned equipment or storage devices to the School computer network or to any School-owned equipment, whether on the School's network or not.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I agree to abide by all the points above.

Signature Date

Full Name (printed)

I would like permission to connect the following personal equipment on the school network and/or school-owned equipment:

Headteacher approval: Yes / No

Signed _____ Date _____