Whitwick St. John the Baptist C.E. Primary School

E-Safety Policy

Agreed by Staff: **June 2021**
Agreed by Governors: **June 2021**

Signed (Chair): _____ Date: _____

Contents

Appendices

1. Introduction

1.1 **Whitwick St. John the Baptist C.E. 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 **Whitwick St. John the Baptist C.E. 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 disabled 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 the headteacher.

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 Whitwick St. John the Baptist C.E. 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 Whitwick St. John the Baptist C.E. 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 Schools Broadband Team who provide a managed (not 'locked down') network system. We fully support and will continue to work with schools broadband 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.

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 policies and 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 Whitwick St. John the Baptist C.E. 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.

<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

[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, PDAs etc.

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 school broadband or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves schools broadband or members of 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 schools broadband, or to schools broadband 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 schools broadband 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 schools broadband 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 schools broadband has requested that use cease because it is causing disruption to the correct functioning of schools broadband.
  - other misuse of the schools broadband 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 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 Definition of Abuse

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

4.3 Reporting Abuse

4.3.1 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.

4.3.2 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 Safeguarding Lead for Child Protection within the School will refer details of an incident to Children's Social Care or the Police.

[2] Chapter 9 of the LSCB Procedures

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 Whitwick St. John the Baptist C.E. 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.
- Audit 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

Whitwick St. John the Baptist C.E. Primary School recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

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

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 .

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, Whitwick St. John the Baptist C.E. 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.

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 This policy statement should be read alongside our organisational policies and procedures for both staff and pupils, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance
- ICT equipment (onsite and offsite)
- GDPR, data security and retention.

Appendix A:

General Information for Staff (Staff Handbook) *[extract]*

Use of ICT

In accordance with data protection regulations, ALL staff should ensure the security of data. This could be the use of passwords for computers (laptops and PCs) and any memory storage devices. Access to data should be restricted to authorised persons only. Disclosure should only be in accordance with their professional duties. Data containing names and personal details of children should only be stored on an encrypted memory storage device and should not be saved on the hard drive of teacher laptops.

Copyrighted software should not be made available outside of the establishment. If uncertain about school licences, please contact a member of the office staff.

Software should not be copied onto school pcs or laptops without prior permission of the headteacher. Anti-virus protection should be installed and maintained on all computer equipment. Staff should notify the ICT technician when it is due for update or if in doubt of its current status. A copy of the ICT policy can be obtained from the office.

Internet Use

The school Admin and Curriculum network is protected by Schools Broadband firewalls which block inappropriate websites and emails. However, children should be supervised when using the internet to research information. Please refer to the ICT policy for further clarification. Staff should follow the school's E-Safety guidance.

Staff must ensure that they adhere to the Internet Acceptable Use Policy and must not access social media sites for personal reasons during working time.

Social Media Sites

All employees are expected to adhere to the "use of social media sites" policy at all times. Employees must ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

Social media sites include: Facebook, My Space, Twitter and Instagram but are not limited to just these.

Mobile Phones

All employees are expected to switch off their mobile phones during lesson times. Mobile phones should not be used under any circumstances to photograph or record children. In the event of any emergency, please ask your contacts to call the school office.

Staff are expected to renew their signed agreement annually.

Appendix B:

Whitwick St John the Baptist CE Primary School Internet and ICT Acceptable Use Policy for Staff and Volunteers

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users.
- I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems including email and other digital communications technologies.
- I understand that this agreement also apply to use of school ICT systems out of school (e.g. laptops, email, VLE etc.).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, to the appropriate person in school.
- I will be professional in my communications and actions when using school ICT systems: I will not access, copy, delete or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's policy. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify pupils by name, or other personal information.
- I will only use chat and social networking sites in school in accordance with school policy.

- I will only communicate with pupils and parents / carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email address). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

Use of ICT

In accordance with data protection regulations, ALL staff should ensure the security of data. This could be the use of passwords for computers (laptops and PCs) and any memory storage devices. Access to data should be restricted to authorised persons only. Disclosure should only be in accordance with their professional duties.

Data containing names and personal details of children should only be stored on an encrypted memory storage device and should not be saved on the hard drive of teacher laptops.

Copyrighted software should not be made available outside of the establishment. If uncertain about school licences, please contact a member of the office staff.

Software should not be copied onto school pcs or laptops without prior permission of the headteacher.

Anti-virus protection should be installed and maintained on all computer equipment. Staff should notify the ICT technician when it is due for update or if in doubt of its current status.

Staff Internet and Mobile Phone User Agreement

Internet Use

The school Admin and Curriculum network is protected by schools broadband firewalls which block inappropriate websites and emails. However, children should be supervised when using the internet to research information. Staff should refer to the ICT policy for further clarification. Staff should also follow the school's E-Safety guidance.

Staff must ensure that they adhere to the Internet Acceptable Use Policy and must not access social media sites for personal reasons during working time.

Social Media Sites

All employees are expected to adhere to the "use of social media sites" policy (a copy can be obtained from the office) at all times. Employees must ensure that they conduct themselves in a manner that will not place children or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

Social media sites include: Facebook, My Space, Twitter and Instagram but are not limited to just these.

Mobile Phones

All employees are expected to switch off their mobile phones during lesson times. Mobile phones should not be used under any circumstances to photograph or record children. In the event of any emergency, please ask your contacts to call the school office.

Staff are expected to renew their signed agreement annually.

Appendix C:

Whitwick St John the Baptist CE Primary School
Acceptable Use Policy for Primary Pupils

Please talk to your child about keeping safe on the internet, ensuring they are aware of the school's policy:

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules

- I understand that the school's behaviour guidelines will be followed

Further internet safety guidance can be found on e-schools.

My parents/carers have spoken to me about the school's internet and email policy and I agree to follow it.

Name of pupil _____

Signed _____ Date _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature _____ Date _____

Appendix D:

Data Security and retention, Back-up procedures and Disaster recovery

School data is backed up remotely to the LEAMIS service at County Hall.

The school has a business continuity plan which can be accessed from the school office.

Appendix E:

Internet and email

All staff and pupils are supplied with a school outlook email account.

Appendix F:

Access and Privacy

The school's computers should not be used at any time for downloading, copying or storing illicit or offensive material, nor should video, music or other files which take up a large amount of space be stored on our servers. Users wishing to download and copy large files to a

should discuss it with the ICT Coordinator.

No user should attempt at any time to install any software of any kind onto the school network or onto any workstation connected to it, including screensavers. If a member of staff wishes to have software installed the agreement of the ICT Coordinator or headteacher should first be sought, the licence checked and the relevant media handed to the ICT Coordinator to arrange for installation.

All users of the network must be aware that their user areas and individual files may on occasion be accessed by the network administrators and files which contravene any part of this policy may be removed.

All use of the school's ICT resources should be in line with this policy and the rules laid out in the school's Acceptable Internet Use Policy.

Appendix G:

Social Networking Policy

(For pre-school staff and parents of children who attend Penguin pre-school
and Whitwick St John the Baptist C of E Primary School)

Staff already follow the rules laid down by the councils 'social networking policy'.

This includes items such as the legality of comments that are/are not acceptable to
be made on internet sites such as 'Twitter' and 'Facebook' and safeguarding issues that can arise from inappropriate friendships etc.

Whilst we cherish and value the close relationship we have with the parents and families of the children who attend/have attended our pre-school, we also have a duty to be professional in our roles of practitioners in a teaching establishment.

Parents are individuals with a private life, as are the staff. In order to help establish and clarify the clear line between personal and professional roles between parents/families and pre-school staff, we felt it appropriate to generate the following rule.

Staff, apprentices, placement and work experience volunteers may not seek out, 'add' or send friend requests to parents of children or children who attend Penguin Pre-school or Whitwick St John the Baptist C of E Primary School. Requests made to all those stated above by parents must be declined. This rule applies whilst all are employed within the Pre-school, school or during their time of placement.
When staff are friends with parents previous to starting their placement or employment contract, they should disclose this to the Head teacher at the earliest possible time. They should then follow the previous guidance and not 'add' any other parents.
When staff are also parents of children at school or Pre-school, they should discuss with the Headteacher whether it is appropriate for links to be made on social media with other parents. An example of an acceptable use would be, the use of social media to keep up to date with a sports group that their child belongs to that other parents also use although there may be other examples of use that are deemed acceptable. If any employee of either the School or pre-school are in any doubt of a situation, they should neither accept a parent's friend request or communicate with them online until a consultation with headteacher has taken place and a decision has been made. If headteacher deems that it is an acceptable use, then the staff member should still be conscious of the other agreements they have made when signing the Acceptable use policy and also not make contact with the parent for any reasons other than those which were agreed upon. Should headteacher deem it to be an unacceptable use, then the staff member is required to decline the request as soon as it is convenient to do so.
School staff and pre-school staff may be 'friends' with each other on social networking sites (even if they have children within the pre-school/school) as they already follow the protocols set down by the schools social networking policy.
As always we encourage all parents to approach staff in person, by letter or phone call and will continue to strive to always be available should you need support or help in any way. All staff must ensure that they follow the acceptable use policy.

Appendix H:

Leicestershire County Council: Personal Use of Social Media Sites Policy and Procedure [See LCC document]: