Blyton cum Laughton Church of England Primary School

E-Safety & Acceptable Use Policy

Monitoring responsibility	K Duke (Headteacher)
Review date	October 2017
Head teacher's signature	
Chair of Governor's signature	
Date ratified	October 2018

1. BACKGROUND

1.1 While digital technology can be used in positive ways, it can also be used in extremely negative ways. Paedophiles may use this technology to contact, groom and blackmail young people in the virtual world with a view to abusing them in the real world, children and young people are able to anonymously bully classmates and teachers, while adults may find themselves at greater risk of identity theft should they publish too much information about their life onto a social network.

1.2 The risks are real but many people do not see that activity within a virtual world can have an effect in the real world. Comments posted onto social networking sites have led to staff being disciplined and young people being bullied. Many are also unaware that some activities in the virtual world are criminal offences and can lead to prosecution.

1.3 The Lincolnshire Safeguarding Children Board has overall statutory responsibility for the safeguarding of the child, and that includes the virtual world as well as the real, and takes seriously the role it has to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in the locality, and to ensure that they are effective in doing so.

1.4 Primarily e-safety is used to describe pro-active methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to remain safe we should educate them not only in the dangers but also inform them who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well researched good practice and continuing development. (Lincolnshire Schools E-Safety Policy and Guidance – June 2010).

2. ROLES AND RESPONSIBILITIES

2.1 The Headteacher will ensure that:

2.1.1 All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
2.1.2 The Designated Teacher for safeguarding receives appropriate on-going training, support and supervision.
2.1.3 All temporary staff and volunteers are made aware of the school's E-learning/Safety Policy and arrangements.
2.1.4 A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
2.15 All members of staff have a school email address.

2.2. The Governing Body of the School will ensure that:

2.2.1 This policy is applied correctly for E-Learning/Safety within the school.
2.2.2 Procedures are in place for dealing with breaches of E-safety and security and are in line with Local Authority procedures.

2.3 The Designated Teacher for safeguarding will:

2.3.1 Act as the first point of contact with regards to breaches in E-Safety and security.
2.3.2 Receive appropriate training.

2.3.3 Provide support and training for staff and volunteers on E-Safety.
2.3.4 Ensure that all staff and volunteers have received a copy of this policy.
2.3.5 Ensure that all staff and volunteers understand and are aware of the school's E-Learning/Safety Policy.
2.3.6 Ensure that the school's ICT systems are regularly reviewed with regard to security.
2.3.7 Ensure that the virus protection is regularly reviewed and updated.
2.3.8 Discuss security strategies with the Local Authority particularly where a wide area network is planned.
2.3.9 Regularly check files on the school's network.
2.3.10 If there is any suspicion of illegal activity, NEVER investigate themselves, but must report to Lincolnshire Police as soon as possible.

2.4 All staff will:

2.4.1 Read this document, including relevant appendices. Staff thereby accept that the school can monitor network and internet usage to help ensure staff and pupil safety.
2.4.2 Report anything inappropriate that they find on the school internet to the Headteacher immediately.
2.4.3 Confiscate items such as mobile phones, ipods, ipads etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy (Education and Inspections Act 2006).

3. Teaching and Learning

3.1 Benefits of using the internet in education include:

3.1.1 Access to world-wide educational resources
3.1.2 Educational and cultural exchanges between pupils world-wide;
3.1.3 Access to experts in many fields for pupils and staff;
3.1.4 Staff professional development through access to national developments, educational materials and good curriculum practice;
3.1.5 Communication with support service, professional association and colleagues;
3.1.6 Improved access to technical support including remote management of networks;
3.1.7 Exchange of curriculum and administration data with the LA and DfE
3.1.8 Ability for parents to support child's home learning;

3.2 The school internet access will be designed expressly for pupils use and include filtering appropriate to the age of pupils.
3.3 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
3.4 Internet access will be planned to enrich and extend learning activities.
3.5 The School's E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.
3.6 It should be remembered that digital technology reaches far and wide, not only computers and laptops, but consideration should also be given to technologies such as: Ipads, Ipod Touches and Iphones; Xbox 360, Playstations, Nintendo Wii, mobile phones and PDA's, and anything else which allows interactive digital communication.

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

4. Staff use of Internet

4.1 Use of the internet on school premises should principally be for school use, e.g. accessing learning, resource, educational websites, use of mail etc.
4.2 Websites used will be viewed by the staff member prior to the lesson, with regular checks being made of the internet browser
4.3 Staff should not be accessing the internet for personal reasons while teaching children
4.4 Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. (If accessed accidentally users should report the incident immediately to the Headteacher)
4.5 Children will be made aware of the action to take if they find something that makes them feel uncomfortable or upset.
4.6 The school recognises that many staff will actively use Facebook, Twitter and other such social networking sites. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their or any other member of staff suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks.
4.7 It is never acceptable to accept a 'friend request' from pupils, as in almost all cases children of infant age using networks will be breaching terms and conditions of use of those networks. It is never acceptable to initiate a friend request with a pupil. It is inadvisable to accept friend requests from ex-pupils. It is inadvisable for staff to accept or initiate a friend request with a parent or carer on social networking sites. Setting a high security level on social networking sites is highly advised.

5. Passwords

5.1 Staff should keep passwords private. Passwords are confidential and individualised to each person. Children should not be using a computer that is logged on to a staff member's account. If this is essential there must be 1:1 supervision.

6. Data Protection

6.1 All sensitive data, such as children's details and reports, should be kept on machines where a password is needed to access. Staff members may take home files such as reports, but these must be used appropriately. It is advised that if these are taken off school site they are saved on a password protected laptop/computer.

7. Images and Videos

7.1 Staff and pupils should not upload onto any internet site school images or videos of themselves or other staff or pupils without consent.

8. Mobile Phones

8.1 Mobile phones should not be used when teaching, unless in an emergency, but permission must be sought from the Headteacher. They should only be used in the staff room or before children have arrived in school or left the school.

9. Viruses and other malware

9.1 Any virus outbreaks are to be reported to the Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Associated Policies:
Safeguarding/Child Protection
Staff Code of Conduct
Induction Policy

Review

This policy will be reviewed annually by the Headteacher and Governing Body of Blyton cum Laughton CE Primary School.