

# E-safety Policy



**The Grange Primary School**

July 2016  
Review date: Autumn 2019

## Contents

1. Introduction
2. How Internet use benefits children at The Grange Primary School
3. How we ensure Internet use enhances learning and life experiences at The Grange Primary School
4. How information systems security will be maintained at The Grange Primary School
5. How filtering is managed at The Grange Primary School
6. How video conferencing is managed at The Grange Primary School
7. How Personal data is protected at The Grange Primary School
8. Password security at The Grange Primary School
9. How Email is managed at The Grange Primary School
10. How published content is managed at The Grange Primary School
11. How social networking is managed at The Grange Primary School
12. How Internet access is authorised
13. How risks will be assessed at The Grange Primary School
14. How complaints will be handled at The Grange Primary School
15. How the Internet and E-safety will be used across the community
16. How Cyberbullying will be managed at The Grange Primary School
17. How The Grange Primary School responds to an incident of concern
18. How communication is handled at The Grange Primary School
19. How this policy will be introduced to children at The Grange Primary School
20. How this policy will be discussed with Staff at The Grange Primary School
21. How parent/carers support will be enlisted

### 1. Introduction

The Internet has become increasingly accessible for children and young people in places like schools, libraries and their own homes. Children will experiment online at

home and at school, to enable them to take advantage of the many educational and social benefits of new technologies. Children need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviour.

## **2. How Internet use benefits children at The Grange Primary School**

The Internet is an essential element in 21<sup>st</sup> century life. ICT skills and knowledge are vital to access life-long learning and employment, indeed ICT is now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All children and young people should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to children and young people and the professional work of staff, for example:

- access to world-wide educational resources,
- access to experts in many fields,
- educational and cultural exchanges between children and young people worldwide,
- collaboration and communication within the wider context,
- access to learning wherever and whenever convenient.

The Internet enhances the management information and business administration systems for example within:

- communication systems;
- improved access to technical support, including remote management of networks and automatic system updates;
- online and real-time 'remote' training support;
- Secure data exchange between local and government bodies.

## **The Risks**

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for Children and young people. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

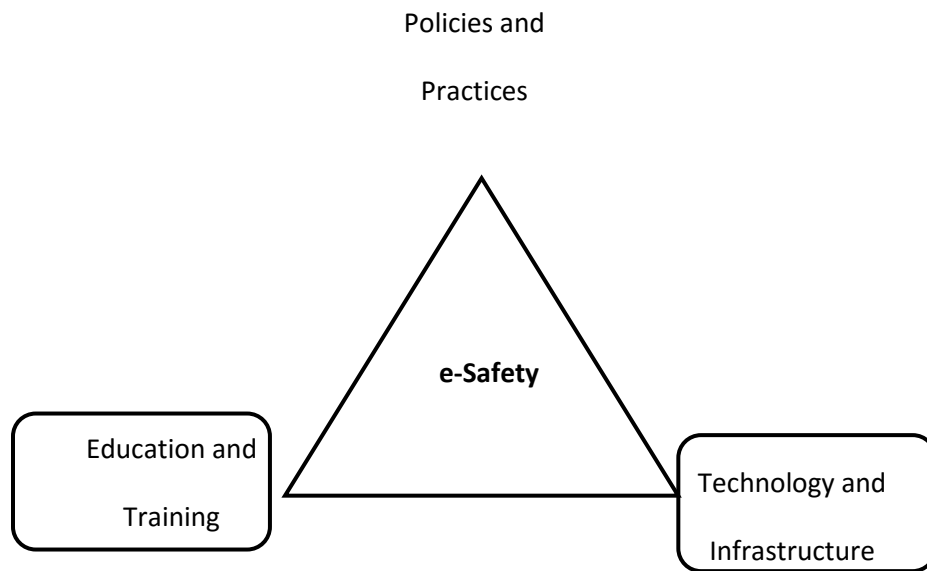
In line with policies that protect children and young people from other dangers, there is a requirement to provide as safe an Internet environment as possible and to teach children and young people to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture. The internet can pose risks and people working with children and young people should consider extending an education programme to parents and carers.

There are decency laws in relation to computer technology. It is a criminal offence to hold images of child abuse on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening emails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Agencies working with children and young people need to make it clear that using equipment to view or transmit inappropriate material is "unauthorised" and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken. Reasonable steps include technical and policy actions and an education programme for children, young people, staff, and parents.

There are three core elements for an organization to address when considering e-safety:

- Technology
- Policy and Practices
- Education and training



### **3. How we ensure Internet use enhances learning and life experiences at The Grange Primary School**

The Grange Primary School's Internet access will be designed to enhance and extend education. Children will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use. Staff at The Grange Primary School will ensure that the copying and subsequent use of Internet derived materials by staff and children complies with copyright law. Staff will guide children to on-line activities that will support the learning outcomes planned for their age and maturity. Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **4. How information systems security will be maintained at The Grange Primary School**

Security at The Grange Primary School is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff, children and young people. The named person in charge of Data Security at The Grange Primary School is Mrs Larissa Thorpe (The Business Manager). All staff at The Grange Primary School with access to personal data understands that they are liable in law to protect that data. Should data be lost from an unencrypted USB drive or seen on a laptop used by other people, staff understand that the

consequences could be serious for the member of staff and for the school. Staff use encrypted memory sticks to transport any such data between home/school.

Access to all ICT systems within the school and laptops that are taken home can only be accessed by a unique login and password for the individual. All requests for access beyond that normally allocated (e.g. teachers wishing to access pupil personal storage) are authorised by the person in charge of data security. This includes the authorisation of access required by the ICT Support Team, Osborne Technologies. Where 'restricted' information is stored in SIMS or the server, access is only granted to individuals approved by the person in charge of data security, Mrs Larissa Thorpe (The Business Manager).

Workstations are secured against user mistakes that compromise access or security and deliberate actions - Lock screen is used. Servers securely locked and physical access restricted. Virus protection from Sophos for the whole network is installed and current. Access by wireless devices is pro-actively managed and is password protected.

#### **5. How filtering is managed at The Grange Primary School**

Levels of Internet access are consistent across the school for children and staff separately, and access profiles are to a level appropriate for all members of the organisation. Children or visitors to the school have no access to restricted websites. The Grange Primary School manages the filtering systems locally within the school and ensures that systems to protect children and young people are reviewed and improved regularly. Broadband access includes filtering appropriate to the age and maturity of children. Regular requests for filtering changes from within the organisation are made via Mrs Deb Bibby, Schools' ICT Instructor. Mrs Deb Bibby also ensures that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

#### **6. How video conferencing is managed at The Grange Primary School**

Video conferencing is an embedded technology at The Grange Primary School. All video conferencing equipment will be switched off when not in use and not set to auto answer. Video conferencing contact information will not be put on the school Website. Video conferencing will always be adult supervised. Unique log on and password details for the videoconferencing services will only be issued to members of staff and kept secure.

All children will be reminded before video conferencing commences that they must not disclose their surname or other personal details.  
Parent/Carer permission will not be required for video conferencing as permission is given on the school admission form.

## **7. How personal data is protected at The Grange Primary School**

The quantity and variety of data held on children, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Grange Primary School fully complies with The Data Protection Act 1998.

## **8. Password Security at The Grange Primary School**

All staff and children at The Grange Primary School understand the importance of keeping their passwords secure from others. The Grange Primary School recommends to all staff to use a different password for accessing organisational systems to that used for personal (non-organisational) purposes. When leaving a computer for any length of time, all staff members/volunteers are told to log off or lock the computer, using CTRL+ATL+DELETE.

Passwords have been introduced to children to access the server from 2016 in year 3 & year 4 and will filter through as each year come through the school.

## **9. How email is managed at The Grange Primary School**

Children will only use approved email accounts and will immediately tell an adult if they receive offensive email. Children will not reveal personal details of themselves or others in email communication.

Staff are provided with a school email address that they can use if they feel it is appropriate.

## **10. How published content is managed at The Grange Primary School**

The contact details on the website are the main address, email and telephone number for the school. No other personal contact information will be published, including the use of children's full names. Children's faces will be blurred out.

Mrs Thorpe takes overall editorial responsibility and ensures that content is accurate and appropriate. Parents/Carers are given regular reminders on the termly newsletter about appropriate content on the Website.

The website complies with all guidelines for publications including respect for intellectual property rights and copyright.

## **11. How social networking and personal publishing is managed at The Grange Primary School**

All adults have been made aware of the potential risks of using social networking sites or personal publishing, either professionally with children and young people or personally. They have been made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Children have been advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory when using the Internet at school or home.

## **12. How Internet access is authorised**

The Grange Primary School maintains a current record of all staff/volunteers and children who are granted access to the organisation's electronic communications. All staff/volunteers read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resources.

For younger children, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials. However, during independent time children can access the internet independently.

Every child and adult in the school will agree to comply with and sign the Acceptable Use Policy. Parents/carers will be informed that children and young people will be provided with supervised and unsupervised Internet access, but must comply with the Acceptable Use Policy at all times.



### **13. How risks will be assessed at The Grange Primary School**

The Grange Primary will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. The Grange Primary cannot accept liability for the material accessed, or any consequences resulting from Internet use. The Grange Primary will audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

### **14. How complaints will be handled at The Grange Primary School**

Parents, staff and children know how to use The Grange Primary’s’ complaints procedure by clicking on the CEOP report abuse button if there is a problem.

Internet related. Children know they can speak to any member of staff across the school if they have any issues or they can speak to the Well-being representative, Miss Baker. Potential child protection and illegal issues will be referred to the Child Protection Co-ordinator and E–safety Co-ordinator. The 'Response to Risk Flowchart' for reporting e-safety incidents will be followed. Any complaint about staff misuse will be referred to the E-safety Co-ordinator. All e–safety complaints and incidents will be recorded by Mrs Bibby — including any actions taken. Children and parents will work in partnership with The Grange Primary to resolve any issues.

### **15. How the Internet and e-safety will be used across the community**

The school will liaise with local organisations (including Primary Technologies) to establish a common approach to e–safety. The ICT co-ordinator, Mrs Bibby, will attend any e-safety related courses to remain up-to-date with any developments. The school will be sensitive to Internet related issues experienced by children and young people out of school, e.g., social networking sites, and offer appropriate advice when needed.

## **16. How Cyber bullying will be managed at The Grange Primary School**

Cyber bullying (along with all forms of bullying) will not be tolerated at The Grange Primary School. Full details are set out in The Grange Primary School policy on anti-bullying. There are clear procedures in place to support anyone affected by cyber bullying. All incidents of cyber bullying are reported to Miss Baker and will be recorded.

Sanctions for those involved in cyber bullying will include:

\*Internet access may be suspended for the user for a period of time.

\*Parents/carers will be informed.

## **17. How The Grange Primary School responds to an Incident of Concern**

An important element of e-safeguarding at The Grange Primary is the ability to identify and deal with incidents of concern and those related to the confidentiality of information. All staff/volunteers and children know that they have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any adverse impact. The Grange Primary School has an incident reporting procedure and records reported incidents in an Incident Log.

The Incident Log will be kept Miss Baker and will be reviewed annually by the Governing Body.

The children and staff at The Grange Primary School understand and know how to use the 'Hector Dolphin' internet safety button (introduced as part of E-safety Mark).

## **18. How Communication is handled at The Grange Primary School**

The Grange Primary School will include appropriate communication and training for all people (children and adults alike).

This will cover:

- Workforce training in understanding the rationale for all e-safeguarding procedures and the consequences of inappropriate practice.
- Workforce training in responsible approaches to data on mobile devices, communicating online and procedures when using multimedia digital content such as

photographs, videos and podcasts in terms of permission seeking, taking, storage and retention.

- A comprehensive and developmental e-safety curriculum for children including the responsible use of web and communication technologies both inside and outside school and risks related to cyberbullying.
- Annually re-visiting of the AUP with staff and pupils.
- Ensuring non-teaching staff are trained and up-to-date in their subject knowledge
- Up-to-date Acceptable Use Policies (AUPs) based on all the agreed procedures for e-security and e-safety and covering ICT usage by all sectors of the organisational community. This policy shall be subject to annual review by the governing body.

### **19. How this policy will be introduced to children at The Grange Primary School**

A copy of the e-safety policy has been attached to the acceptable use policy for all staff and parents to be aware of its contents and discuss with children how they feel it is appropriate (check with office this is happening). The school as a whole regularly teaches e-safety as part of dedicated ICT e-safety lessons, as part of the IPC topic work and as part of PSHE. The 'Think You Know' and 'CEOP' documents have been used by every class across the school. Before children access the Internet, safe and responsible use of the internet and technology is reinforced.

### **20. How the policy be discussed with staff at The Grange Primary School**

The E–safety Policy has been formally provided to and discussed with all members of staff. To protect all staff and children, The Grange Primary School has implemented Acceptable Use Policies, which are being signed every year by all staff, children, volunteers and parents. Staff are aware that Internet traffic can be monitored and traced to the individual user - discretion and professional conduct is essential. Osborne Technologies who manage the schools' filtering systems are regularly supervised by Mrs Bibby, the schools' ICT Co-ordinator.

When staff are provided with digital devices (e.g. laptops, camera) by The Grange Primary School that may be accessed outside of the organisational network, staff are clear about the safe and appropriate use of the provided equipment and rules about use of the equipment by third parties. Staff are clear that they should not use any

personal devices to take pictures of the children. Staff are aware of their responsibility to maintain confidentiality of the organisation's information. All staff within The Grange Primary School, including administration staff and governors, is included in awareness raising and training. Induction of new staff/volunteers includes a discussion of the organisation's e-safety Policy.

## **21. How parents/carers support will be enlisted**

Internet use in children's homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents/carers are aware of the dangers, children and young people may have unrestricted and unsupervised access to the Internet in the home. The school has helped parents/carers plan appropriate supervised use of the Internet at home and has educated them on the risks by providing an 'E-safety Parents' Awareness Day', with follow-up information for those unable to attend. Parents'/carers' attention has been drawn to The Grange Primary School E-safety Policy by providing them with a copy of this policy annually, along with a copy of the appropriate Acceptable Use Policies.

Agreed By Governors on: \_\_\_\_\_

Governors Signed : \_\_\_\_\_

Head Teacher signed : \_\_\_\_\_