William Austin Junior School
Policy for Online Safety

Introduction
The Internet is an essential element in 21st century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As such, the school has a duty to provide pupils with quality Internet access as part of their learning experience.

At William Austin Junior School we believe that the use of information and communication technologies in school brings great educational benefits. However, we recognise the Online Safety issues and plan accordingly to ensure appropriate, effective and safe use of electronic communications.

Luton Borough Council provides Internet access for our school, which is designed for pupil use and includes filtering appropriate to a junior school.

This policy should be used in conjunction with the school's policy for Safeguarding which details child protection procedures.

Writing and reviewing the Online Safety policy

Our Online Safety Policy has been written by the school and agreed by Senior Management.
The Online Safety Policy is part of the ICT Policy and School Development Plan and relates to other policies including those for behaviour, personal, social, health, citizenship and economic education (PSHCEE).

- The appointed Online Safety Coordinators are: the Computing Co-ordinator and ICT technician
- The Online Safety Policy will be monitored by the Safeguarding Governor

1. **Teaching and learning**

The importance of Internet use

- The purpose of Internet use in school is to raise educational standards, enhance learning and prepare our pupils for secondary and further education and their working life.
- Internet use is also a necessary tool to support the professional work of staff and to enhance the school's management functions.
- Pupils are taught what Internet use is acceptable and what is not, and are given clear objectives for its use.
- Pupils are educated in the effective use of the Internet for research, including the skills of knowledge location, and retrieval.
- Pupils are taught to evaluate Internet content, including how to identify various aspects of websites such as adverts and offsite links and to know that information can be biased.
- Pupils are taught the importance of cross checking and validating information before accepting its accuracy.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to report unpleasant Internet content to their teacher, the Computing Lead Teacher or the ICT Manager/Technician.
- Pupils are taught the importance of, and how to stay safe online, including password security and protection of personal information.

The benefits of the Internet for teaching and learning

Broadband Internet use within school and the Learning Platform provide enhanced opportunities for teaching and learning, including:

- access to world-wide educational resources including museums and art galleries;
- shared learning resources which can be accessed online, outside lesson time and from any location;
- vocational, social and leisure use in libraries, clubs and at home;

- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- access to school materials offsite.

2. Managing Information Systems

Network security issues

System security includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions – staff will change generic passwords to secure personal passwords.
- Servers are located securely and physical access restricted – the ICT room, server cupboards and school office will be locked outside of school hours.
- The server operating systems are secured and kept up to date – the Computing Lead Teacher and ICT Manager/Technician have administrative access to the Curriculum server
- Members of the teaching staff have access to areas of the network which allow them to store and edit teaching and learning materials
- Virus protection for the whole network is installed and updated regularly.
- Access by wireless devices is pro-actively managed.
- Access to personal data on home networks is restricted for use by professionals only;
- External devices are screened before use and are prohibited from access to the system.

Managing e-mail

- A messaging buddy system will be developed within our own school to enable pupils to begin to use e-mail and instant messaging technology to communicate and share information.
- Pupils will only be issued with user names and passwords, and allowed to use e-mail and instant messaging technology once they have been taught the Online Safety Code of Conduct and the reasons for these rules.
- Pupils will learn to send e-mail and instant messages as part of a planned lesson and will have the content they compose checked by a member of staff.
- In-coming e-mail and messages to pupils will not be regarded as private.
- Pupils must immediately tell a teacher if they receive offensive e-mail or message.
- Pupils should not be permitted to reveal personal details of themselves or others in e-mail or instant message communication, or arrange to meet anyone without specific permission.
- All teaching and support staff are provided with a school email address, which should be used for all work related emails. Staff should not communicate with pupils via email.
- E-mail sent to an external organisation will be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Managing published content on the school website

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on the website.

Managing published content on the Learning Platform

- Pupils will only be issued with user names and passwords, and allowed to use the Learning Platform, once they have been taught the Online Safety Code of Conduct and the reasons for these rules.
- The Learning Platform will remain a secure part of the school website - pupils and staff will need to use their user name and password to access resources.
- Pupils' work will only be published in secure areas of the Learning Platform.
- Access to online discussions and activities, displaying pupil names, will be contained within secure areas of the Learning Platform.

Managing filtering

William Austin Junior School uses Precedence onsite filtering to ensure internet access is appropriate for all members of the school community.

- The filtering strategy is designed to suit the age and curriculum requirements of our pupils
- The school will work with Precedence to ensure systems to protect pupils are regularly reviewed
- The discovery of unsuitable sites of illegal material by staff or student will result in the URL being reported to the Computing coordinator or ICT Manager/Technician, who will alert the appropriate authorities

Managing emerging technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones or any other personal networking devices belonging to pupils are not permitted in school at any time.

Social networking and Online Gaming

Whilst most social networking sites are inappropriate for our children, we are aware that some children will bypass online age restrictions to access these sites. Many of our children are using the internet to play multiplayer games, some of which involve bypassing age restrictions. We will therefore ensure that within our teaching of Internet safety, discussion about the dangers children may encounter in these online spaces will take place.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location e.g. real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Pupils will be advised on security and encouraged to set 'strong' passwords, deny access to unknown individuals, invite known friends only and deny access to others.
- We are aware that bullying can take place through social networking and this is reflected in the Anti-Bullying Policy and is covered within the PSHCEE scheme of work
- Staff will not run social network spaces for student use on a personal basis or communicate with pupils, past or present, through such sites.
- Staff should not make reference to students/parents/staff or issues relating to the school on social media, and any opinions shared must not be attributed to the school.
- Staff must regularly check the security settings on their social media profiles to minimise the risk to their personal data.

3. Policy Decisions

Authorising Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff and pupils must read and sign the 'Online Safety Code of Conduct' before using any school ICT resource.
- Pupils' access to the Internet, for research purposes and to access online material, will be supervised and monitored.
- Parents will be informed that pupils will be provided with supervised Internet access and will be asked to sign and return a consent form.

Assessing risks

- The school 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 school computer. Neither the school nor Luton Borough Council can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that its implementation is appropriate.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with promptly by the Senior Management Team or Computing Lead Teacher.
- Definitions of misuse include (but are not exclusive to) material which is designed to offend, be sexually explicit, linked to extremism / radicalisation or cyber bullying.
- The facts of the case will be established, including whether the Internet use was within or outside school. Potential child protection or illegal issues must be referred to the school Designated Child Protection Co-ordinator or Online Safety Co-ordinator.
- Any complaint about staff misuse will be referred to the Headteacher, or in the case of the Headteacher, the matter will be referred to the Chair of Governors.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions for pupils, within the school discipline policy, will include: interview/counselling by a member of the Senior Management Team or Computing Lead Teacher, informing parents or carers and removal of Internet or computer access for a period.

Internet use across the community

Internet access is available in many situations in the local community e.g. home, local library, youth club etc.

- Where possible, the school will liaise with local organisations to establish a common approach to Online Safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Introducing the Online Safety Policy to pupils

- Online Safety rules will be posted in rooms with Internet access and will be discussed regularly with pupils.
- Pupils will be informed that network and Internet use will be monitored;
- An Online Safety training programme will be undertaken to raise the awareness and importance of safe and responsible internet use, both at school and outside school;
- Online Safety will be incorporated into Computing lessons on a regular basis and in other subject areas where the issue becomes relevant.

Introducing the Online Safety Policy to staff

The Online Safety Policy will only be effective if all staff subscribe to its values and methods.

- Induction of new staff will include the school's Online Safety Policy. All staff will be given the School Online Safety Policy and its application and importance will be explained.
- Staff should be aware that Internet traffic and e-mail data can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who monitors ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

Introducing the Online Safety Policy to parents

- Parents' attention will be drawn to the school's Online Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach towards Online Safety will be encouraged.

This policy will be monitored and reviewed by the Computing co-ordinator on an annual basis.

Policy updated: January 2019

Staff responsible: Kate Bridgland

This policy was ratified by the Governing body on: 6th March 2019

Signed on behalf of the Governing Body: _____(signature)

_____(printed)