ACKLAM GRANGE SCHOOL

E-Safety Policy

2020-2021

Status & Review Cycle	**Term**	**Year**
Last Review Date/Policy Adopted	Summer Term	2019-2020
Next Review Date	Summer Term	2020-2021
Lead	Ms Crawshaw/Mrs Flint/Mr Lodge	

This school is an academy within The Legacy Learning Trust.

The Legacy Learning Trust

Contents

1. Policy Implementation and Oversight

- The school has a Safeguarding Team that includes two members of staff with specific responsibility for E-Safety. They liaise directly with the Designated Safeguarding Lead as and when the roles overlap.
- The E-Safety Policy and its implementation will be reviewed annually.
- Acklam Grange School's E-Safety Policy has been written by the school, building on government guidance. It has been agreed by the Senior Leadership Team and approved by the Local Council.

2. Teaching and Learning

2.1 Why is internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Students use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
- The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

2.2 How does internet use benefit education?

Benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between students worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for students and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

2.3 How can internet use enhance learning?

- The school's internet access will be designed to enhance and extend education.
- Students will be taught what is and isn't acceptable in terms of internet use and given clear objectives for internet use.
- The school will ensure that the copying and subsequent use of internet derived materials by staff and students complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.4 How will students learn how to evaluate internet content?

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject.

3 Managing Information Systems

3.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Documents including sensitive personal data which are sent over the internet or taken off site will be encrypted. Support for this can be provided on request by the IT Service and Development Team.
- If portable media is used for the storage and transportation of school based data it must be virus checked and encrypted. No unapproved software may be executed from portable media.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked; media files that contravene copyright will be removed.
- The IT Service Team Leader will review system capacity regularly.
- Student user areas are provided by the school for students to save files relating to their studies. Students have two storage areas available to them – 'Documents' on the school network and 'OneDrive' cloud storage. These are not private storage areas in the same way a student exercise book is not private. The school reserves the right to review the files stored in student user areas as required.

*****Please refer to the school's Data Protection Policy for further information*****

3.2 How will email be managed?

- Acklam Grange School (AGS) students may only use approved email accounts in school.
- Students must immediately tell a teacher if they receive offensive email. They also have the facility to use the Tootoot web application which allows students to safely report any worries and incidents of bullying, cyberbullying, racism, extremism, radicalisation, sexism, mental health and homophobic issues directly to an appropriate person within school.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an appropriate adult.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- When communicating with Acklam Grange School students, staff should only use the systems provided and managed by the school. These include the VLE (eSchools) and school email accounts. Please refer to the Social Networking Policy for further details.

3.3 How will published content be managed?

- The contact details on the website are the school address, central school e-mail and telephone number. Staff or students' personal information must not be published.

- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. This task will be delegated as appropriate.

3.4 Can student's images or work be published?

- Images that include students will be selected carefully.
- AGS students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.
- AGS students work can only be published externally with their permission or that of the parents.
- Students images may be used within the school as part of a learning activity without parental permission (e.g. a video assessment of a drama piece, photos of an experiment taking place etc.), but images will only be stored on school systems for the period of time that the learning activity requires them and deleted afterwards. Images will not be made available to students outside the group specifically engaged in the planned learning activity.

3.5 How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites from all networked technologies.
- Students will be encouraged to consider the range of risks that are known to be associated with social networking systems. Students will be advised always to limit and carefully manage their privacy settings.
- Students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students should be advised to understand the dangers inherent with placing personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should include an understanding of how the background details in a photograph could identify the student or his/her location.
- Staff official blogs or wikis should be password protected and linked to, or hosted within, the school website with approval from the Leadership & Management Team. Staff are advised that social network spaces for AGS students should only be used for educational purposes.
- Staff are advised that personal social networking and media systems should not be publicly associated with the school and should understand that bringing their profession and/or their employer into disrepute will result in disciplinary proceedings.
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should enable moderation by school staff.
- Professional use of education social media accounts is acceptable, providing that its content and discussions are of an educational nature only.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and be instructed on how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

3.6 How will filtering be managed?

- The school will continually work to ensure that systems to protect students are reviewed and improved.

- If staff or students discover unsuitable sites, the URL must be reported to the Safeguarding Team or the IT Service and Development Team.
- If inappropriate sites have been deliberately accessed the school will initiate disciplinary proceedings and/or sanctions as required. If the sites are potentially illegal or a part of a pattern of behaviour the school will involve appropriate safeguarding, law enforcement and local authority professionals.
- The school's broadband access includes filtering through 'Smoothwall' that is specifically tailored to the needs of the school and which is appropriate to the age and maturity of students.
- The IT Service and Development Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school's access strategy will be designed in consultation with teaching staff to suit the age and curriculum requirements of the students.
- The school monitors students' and staff use of the internet through software that flags up keywords that are used in search engines, websites and browsers (Securus). A screenshot is captured and recorded as evidence. Transgressions are dealt with by the members of the Safeguarding Team with responsibility for E-Safety and passed on to the Designated Safeguarding Lead if appropriate.

3.7 How will emerging technologies and mobile devices be managed?

- Emerging technologies will be evaluated for educational benefit by the IT Development Team before use in school is allowed.
- Staff will be issued with a school phone where contact with students is required.
- Mobile phones should be kept out of sight during the school day. Phones may be used to support learning at the discretion of the teacher. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Should a student or staff member report abusive or inappropriate messages on a personal mobile device the school should (with the owner's permission) photograph the message and follow the school's anti-bullying procedures. Should you suspect that the message is illegal (racist, threatening, etc.) you should isolate the device securely and take advice from the Safeguarding Team.

3.8 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.9 How will the school community be protected from extremism and radicalisation?

- Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people.
- Staff and students are prohibited from accessing any websites or social network pages that promote such views.
- The school has systems and filtering in place to block extremist material and monitor those who attempt to access it.
- Any persons deemed to be accessing extremist material will be reported to the relevant member of the Safeguarding Team (Prevent & Community Cohesion).
- Details of the school's policy on extremism and radicalisation are contained within the Safeguarding & Child Protection Policy.
- Students are made aware of the online dangers in regards to extremism and radicalisation as part of the e-safety provision within curriculum time.

4 Policy Decisions

4.1 How will internet access be authorised?

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications. • All staff must read the 'AGS Digital Handbook' and sign a document to confirm they have read it before using any school IT resource.
- Parents will be informed that students will be provided with supervised internet access, together with guidance of what the school considers to be acceptable use through the Parent/Carer Information Guide.

4.2 How will risks be assessed?

- 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 The Legacy Learning Trust can accept liability for the material accessed, or any consequences resulting from internet use.
- 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.

4.3 How will e-safety incidents be handled?

- Students are made aware of the various means to report an incident. These include:
  - Informing a parent
  - Informing a teacher (e.g. tutor/year leader/subject teacher)
  - Online report via the Tootoot software application (accessed either directly or through a link on the school website.
  - Asking a friend to tell an adult
- Staff are made aware of the signs that might indicate abuse, bullying or harassment.
- If a child or teacher is in immediate danger the school's Designated Safeguarding Lead and Child Protection Officer will be contacted and will decide on the action to be followed.
- If there is concern about the potential illegality of the issue external advice from appropriate professionals will be sought.
- Involvement in online extremist activity or concerns about radicalisation of students will be reported to the member of the Safeguarding Team with responsibility for Prevent & Community Cohesion. Otherwise the school will manage incidents using the schools sanctions as appropriate to the situation. An online activity check may be requested to inform the investigation if deemed appropriate.
- All E-Safety complaints and incidents will be recorded by the school - including any actions taken.
- All incidents involving staff must be referred to the Headteacher.
- Complaints about the school's management of an E-Safety incident will be dealt with under the School's Complaints Procedure.

4.4 How is the internet used across the community?

- The school will liaise with those local organisations with which it is engaged to establish a common approach to E-Safety.
- The school will be sensitive to internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice. If the external activity negatively impacts on the learning of the students in the school, the school will explore appropriate intervention activity.

4.5 How will cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully/bullies, where appropriate, such as examining system logs, identifying and interviewing possible witnesses. Parents will be informed and advised to contact the police and/or the service provider if appropriate.
- Sanctions for those involved in cyberbullying are set out in the school's Anti-Bullying Policy. Please refer to the Anti-Bullying Policy for further details.
- The police will be contacted if a criminal offence is suspected.

4.6 How will the Virtual Learning Environment be managed?

- The IT Development Team will monitor the usage of eSchools, our Virtual Learning Environment (VLE) by students and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised on acceptable conduct and use when using the VLE.
- Only members of the current student, parent/carers and staff community will have access to the VLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.
- When staff, students etc. leave the school their account or rights to specific school areas will be disabled.
- Any concerns with content may be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - The material will be removed by the site administrator if the user does not comply.
  - Access to the VLE for the user may be suspended.
  - Parents/carers may be informed.
- A visitor may be invited onto the VLE by a member of the Senior Leadership Team. In this instance there may be an agreed focus or a limited time slot.

5 Communication of the Policy

5.1 How will the policy be introduced to students?

- All users will be informed that network and internet use will be monitored.
- E-Safety is included within the assembly programme through which students will be made aware of current issues and will be reminded of the importance of safe and responsible internet use. This includes participating in Safer Internet Day each February.
- Student instruction in responsible and safe use shall precede internet access.
- An E-Safety module will be included in the KS3 Computing schemes of learning and progress, covering both safe school and home use.
- E-Safety training forms part of the PRIDE programme across the key stages.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.
- Particular attention will be given where students are considered to be vulnerable.

5.2 How will the policy be discussed with staff?

- The E-Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and students, the school will implement IT Acceptable Use Policies.

- Staff should be aware that internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.
- Staff that manage filtering systems and monitor ICT use will be supervised by the IT Service and Development Manager and have clear procedures for reporting issues. Staff updates on ESafety are issued as and when appropriate.

5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, via email and on the school website.
- A partnership approach with parents is encouraged. This includes:
    - Parent evenings with demonstrations and suggestions for safe home internet use
    - Regular updates and newsletters emailed home.
    - Parent Zone magazines available digitally through the school website.
    - E-Safety training offered to all parents.
- Parents are encouraged to contact school for advice regarding e-safety.