Plantsbrook
LEARNING TRUST

E-SAFETY POLICY

Adopted March 16

E-Safety Policy

Whilst the prime focus of Plantsbrook Learning Trust is to secure the best educational provision for the child, the Trust recognises that the safety, welfare and care of children is paramount. We are therefore committed to the highest standards in protecting and safeguarding the children entrusted to our care at all times. E-safety plays a vital role in safeguarding young people. Safeguarding is defined as:

- Protecting children from maltreatment
- Preventing impairment of children's health or development
- Ensuring that children are growing up in circumstances consistent with the
- provision of safe and effective care; and
- Taking action to enable all children to have the best life chances.

The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This use is achieved across a wide variety of technological platforms. It brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

This policy will cover the following:

Core Principles of Internet Safety

The Internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations. Plantsbrook Learning Trust needs a policy to help to ensure responsible use and the safety of students.
This E-Safety Policy is built on the following five core principles:

Guided Educational Use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become “Internet Wise”. Schools need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Students need to know how to cope if they come across inappropriate material.

Students may obtain Internet access in Youth Clubs, Libraries, public access points and in homes. Ideally a similar approach to risk assessment and Internet safety would be taken in all these locations, although risks do vary with the situation.

Responsibility

Internet safety depends on staff, schools, governors, parents and, where appropriate, the students themselves taking responsibility for the use of Internet and other communication technologies such as phones. The balance between educating students to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. Strategies must be selected to suit Plantsbrook School’s situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant.

Internet Safety Policy

Who will write and review the policy?

Plantsbrook School Internet Policy has been written by Plantsbrook Learning Trust, building on Birmingham Children's Safeguarding Board's advice and guidance and government guidance. It has been agreed by the Leadership Group, Health & Safety Committee, School Council and approved by Governors and the PTA. It will be reviewed annually.

Purpose and scope of the policy

- 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 Plantsbrook School's management information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. Plantsbrook Learning Trust has a duty to provide students with quality Internet access as part of their learning experience.

Benefits of Internet use in education

The benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DfE.
- mentoring of students and providing peer support for them and teachers

How will Internet use enhance learning at Plantsbrook Learning Trust?

- Plantsbrook Learning Trust Internet access is designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line 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.

How will students learn to evaluate Internet content?

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Network Manager or ICT Support.
- Teachers should ensure that the use of Internet derived materials by students and colleagues complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Training will be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.
- Students will be made aware of the term Radicalisation through assemblies, the tutorial program and Think! lessons. They will be made aware of how to keep safe from online influences.

Email

- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and teachers need to maintain vigilance during lessons to prevent it.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

How will Website content be managed?

- The point of contact on the website should be Plantsbrook School and Town Junior School address, school e-mail and telephone number. Staff or students' home information will not be published.
- Students' full names will not be used anywhere on the website.
- Plantsbrook Learning Trust will ensure all photographs used on the school website are in line with the safeguarding policy.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with Plantsbrook Learning Trust's guidelines for publications.
- The copyright of all material must be held by Plantsbrook Learning Trust, or be attributed to the owner where permission to reproduce has been obtained.

Newsgroups and e-mail lists?

Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.

Chat rooms

- Students will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- A risk assessment will be carried out before students are allowed to use a new technology in school.

Managing Internet applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or images is forbidden.
- Sixth Form students have access to a Wi-Fi connection to enable independent study. Students and parents are expected to sign the BYOD (Bring your own device) authorisation forms before access is provided.
- At Plantsbrook Learning Trust Impero will be installed on all computers in school by October 2016. This software allows ICT support staff to identify areas of concern, this can be shared with ACOs and the Senior Leadership team.

Authorisation of Internet access

- Parents will be informed that students will be provided with supervised Internet access
- By using the Internet, students are agreeing to abide by the Responsible Internet Use statement.
- Parents will be asked to sign and return a form stating that they have read and understood the Acceptable use document.

Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. Plantsbrook Learning Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Plantsbrook Learning Trust cannot accept liability for the material accessed, or any consequences of Internet access.
- 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.
- The Headteacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

Filtering

- Plantsbrook Learning Trust will work in partnership with parents, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- Plantsbrook Learning Trust, will manage the configuration of their filtering. This task requires both educational and technical experience.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that Plantsbrook Learning Trust believes is illegal will be referred to the Police, Internet Watch Foundation and CEOP.
- Filtering strategies will be selected by Plantsbrook Learning Trust. The filtering strategy will be selected to suit the age and curriculum requirements of the students.

Student induction

- Rules for Internet access will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHE programme covering both school and home use.

- Assemblies and the tutorial program will highlight the importance of keeping safe online. This covers topics such as Child Sexual Exploitation, Radicalisation, Sexting, Grooming and Cyber-bullying.

Staff consultation

- All staff are governed by the terms of the ‘Responsible Internet Use’ in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with Plantsbrook Learning Trust Internet Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use and on Plantsbrook Learning Trust Internet policy will be provided as required.
- Staff will be made aware of the Social Media guidelines and advised to be aware of their social media practice on both a personal and professional level.

System Security

- Plantsbrook Learning Trust ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with appropriate external consultants, particularly where a wide area network connection is being planned.
- Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in students’ work areas or attached to e-mail.
- Files held on Plantsbrook Learning Trust’s network will be regularly checked.
- The Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Complaints regarding Internet use.

- Responsibility for handling incidents will initially be assessed by the nominated Technician. For minor breaches of the AUP the students will be dealt with in accordance with Whole School Behaviour Policy. For more serious breaches of AUP the matter will be referred to a the senior member of staff with responsibility for ICT who will decide upon the appropriate course of action consistent with the Whole School Behaviour Policy
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and students will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- For students, sanctions available will be consistent with those invoked through the Whole School Behaviour Policy.

Parental Support

- Parents’ attention will be drawn to Plantsbrook Learning Trust’s Internet Policy in newsletters and on the school websites.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This may include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

Community Use

- Adult Education users will need to sign the acceptable use policy.
- Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.

Social Networking Policy

Rationale
The widespread availability and use of social networking applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff at the school.

The purpose of the policy is to:

- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and governors are protected
- Safeguard all children
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

Definitions and Scope
Social networking applications include, but are not limited to:
Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Instagram, and comment streams on public websites such as newspaper sites.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and ICT Policies. Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

Use of Social Networking in practice

1. Personal use of social media/networking

- School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Plantsbrook Learning Trust
- Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection (Ms T Campbell, Mrs N Wigley, Miss L Proctor, Ms H Gould at Plantsbrook School and Ms A Smith, Ms J Gilmour at Town Junior School)
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts

- All email communication between staff and members of the school community on school business must be made from an official school email account
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts
- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

2. School - sanctioned use of social media/networking

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account and several A-level courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- The URL and identity of the site should be notified to the appropriate Head of Department or member of the SLT before access is permitted for students
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.
- Staff should always maintain a formal and courteous and professional tone in communicating with pupils and ensure that professional boundaries are maintained
- Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe.
- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to a member of SLT.
- Staff should not engage with any direct / private messaging with students through social media where the message is not public.
- All social media accounts created for educational purposes should include a link in the About or Info page to the ICT Policy on the school website. This will indicate that the account is officially sanctioned by Plantsbrook Learning Trust.

Potential and Actual Breaches of the Policy

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Plantsbrook Learning Trust Disciplinary Procedure.
- A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Headteacher and Governors will take appropriate action in order to protect the school's reputation and that of its staff, parents, children and anyone else directly linked to the school.

Responsible Internet Use
Rules for Staff and Students

The computer system is owned by Plantsbrook Learning Trust. This Responsible Internet Use statement helps to protect students, staff and Plantsbrook Learning Trust by clearly stating what use of the computer resources is acceptable and what is not.

1. Irresponsible use may result in the loss of Internet access.

2. Network access must be made via the user's authorised account and password, which must not be given to any other person.

3. School computer and Internet use must be appropriate to the student's education or to staff professional activity.

4. Copyright and intellectual property rights must be respected.

5. E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.

6. Users are responsible for e-mail they send and for contacts made.

7. Anonymous messages and chain letters are not permitted.

8. The use of chat rooms is not allowed.

9. The school ICT systems may not be used for private purposes, unless the Headteacher has given permission for that use.

10. Use for personal financial gain, gambling, political purposes or advertising is not permitted.

11. ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

12. The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Adopted March 16

Policy Enforcement

Any breaches of the E-Safety or Whole School ICT Policies will be reported to the Headteacher and further action may be taken. This may amount to misconduct to which the School's Dismissal and Disciplinary procedures apply.

Examples of possible breaches are listed below:-

- Unauthorised, irresponsible or suspected misuse of ICT or the Internet
- Irresponsible use of email
- Communications or content published on social networking sites or websites that could cause damage to the reputation of the School, students, any of its employees or any third party.

Where websites or apps allow the posting of messages online, users must be mindful that the right to freedom of expression applies only to lawful conduct. The School expects that users of social networking apps will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with the terms of use outlined within this policy.

The School will take all reasonable precautions to ensure e-Safety. However, due to the scale and nature of Internet content and the accessibility of mobile technologies, it is impossible to guarantee that unsuitable material will never appear on a School computer or mobile device. The School cannot accept liability for such material, or any consequences from the accessing of it.

Complaints

Our Leader of Learning through ICT, Network Manager and Senior Leadership Team act as first points of contact for any complaints. Any misuse of ICT or the Internet by staff will be referred to the Headteacher.

Complaints of cyber bullying will be dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the School's Child Protection procedures.

Certain incidents may need to be placed on School record, if they relate to bullying or racism.

This Policy has been approved by the Governing Body and is available to parents and the wider community via the School website. The e-Safety Policy is part of the Whole School ICT Development Plan and relates to policies including Whole School ICT, Anti-Bullying, and Safeguarding.