PETERBOROUGH KEYS
ACADEMIES TRUST

E-Safety and Acceptable Use Policy

Version 1.0

October 2022

Trustee Committee: People & Infrastructure
Date Policy Reviewed: October 2022
Date of Next Review: October 2023

Contents

1. About This Policy

1.1 This policy is managed and maintained by the IT Services Manager in conjunction with the School Business Manager, and subject to ratification from the Senior Leadership Team.

1.2 This policy will be approved by the Academy Committee from September 2022.

1.3 Through the development of literacy, numeracy, information and communication technology, enterprise capability, economic and business understanding and financial capability, we have a duty to ensure that all students are able to make a valuable contribution to society and this is impossible to achieve if we do not ensure that students develop and apply their ICT capability effectively in their everyday lives.

1.4 The school is aware of its responsibilities in ensuring that technology usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by all network users.

1.5 Students have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of technology and adopt appropriate practices

1.6 It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1.7 This Policy document is drawn up to help protect all parties – the students, the staff and the school.

The Technologies

1.8 Technology in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information.

Whole school approach to the safe use of Computer based technologies

1.9 Creating a safe ICT learning environment includes three main elements at this school:

(a) An effective range of technological tools;

(b) Policies and procedures, with clear roles and responsibilities;

(c) A comprehensive e-Safety education programme for pupils, staff and parents.

2. Roles and Responsibilities: Overview

2.1 E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of the Governing Body, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy is monitored. The responsibility for e-Safety has been designated to a member of the school's management team.

2.2 Our Trust e-Safety Co-ordinator is Andy Hudson.

2.3 Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Headteacher, Senior Leadership Team and Local Governing Body are updated as necessary.

2.4 Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated where appropriate on policy developments.

2.5 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

2.6 All staff should be familiar with the school Policy. They accept the Policy on a daily basis when they access the School's Network. The complete Policy is available on the School VLE (Firefly) and in the Staff Handbook. Induction for the use of the Network is provided by the IT Services Manager as CPD. The following items are included:

(a) Safe use of e-mail;

(b) Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;

(c) Safe use of school network, equipment and data;

(d) Review of the GDPR and how it affects the way we handle personal data and protections we put in place to keep personal data safe;

(e) Safe use of digital images and digital technologies, such as mobile phones and digital cameras;

(f) eBullying / Cyberbullying procedures; and

(g) their role in providing e-Safety education for pupils.

2.7 The School includes e-safety in the curriculum and ensures that every pupil has been educated about safe and responsible use. Pupils know how to contrail and minimise online risks and how to report a problem.

2.8 The School makes every effort to engage with parents over e-safety matters.

3. Roles and Responsibilities : Students

3.1 Students are very familiar with the culture of new technologies, and can be involved in designing the School e-Safety Policy, through a student council. Student perceptions of the risks may not be mature therefore the e-safety rules are explained and discussed.

3.2 E-safety is taught as an ICT lesson activity and part of the pastoral programme.

3.3 Instruction in responsible and safe use precedes Internet access.

3.4 An e-safety module is included in the PSHE and ICT programmes covering both school and home use.

4. Roles and Responsibilities : Staff

4.1 It is important that all staff feel confident to use new technologies in teaching. Staff shall be given opportunities to discuss the issues and develop appropriate teaching strategies

4.2 Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

4.3 ICT use is widespread and all staff including administration, Support Staff, Governors and Volunteers are included in appropriate awareness raising and training. This is part of CPD and Induction of new staff.

4.4 Staff are made aware that Internet traffic is logged and can be traced to the individual user. Discretion and professional conduct are essential.

4.5 Staff that manage filtering systems or monitor ICT use will be supervised by a member of the school's senior management and have clear procedures for reporting issues.

4.6 Staff training in safe and responsible Internet use and on the school e Safety Policy will be provided as required.

5. Roles and Responsibilities: Parents

5.1 Internet use in students' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school will try to help parents plan appropriate supervised use of the Internet at home.

5.2 Internet issues will be handled sensitively, and parents will be advised accordingly.

5.3 A partnership approach with parents will be encouraged.

5.4 Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

6. Complaints Regarding e-Safety

6.1 The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Peterborough Keys Academies Trust can accept liability for material accessed, or any consequences of Internet access.

6.2 Staff and pupils are given information about infringements in use and possible sanctions.

6.3 Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

6.4 Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school Safeguarding & Child Protection Policy in conjunction with Trust and Local Authority child protection procedures.

7. Managing the Internet Safely

7.1 Jack Hunt School:

(a) Utilises an educational internet connection managed by e2bn;

(b) Uses Smoothwall Internet Security System to protect our students, staff and systems against dangers from the internet;

(c) Employs Lightspeed content filtering for filtering student mobile devices at home;

(d) Ensures network health through use of Sophos anti-virus software;

(e) Uses individual, audited log-ins for all users;

(f) Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;

(g) Uses teacher 'remote' management control tools for controlling workstations within ICT suites and breakout areas / viewing users / setting-up applications and Internet web sites, where useful;

(h) Has additional local network auditing software installed (currently NetSupport DNA); and

(i) Works in partnership with the Local Authority to ensure any concerns about the system are communicated so that systems remain robust and protect students.

8. Policy and Procedures

8.1 Jack Hunt School:

(a) Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;

(b) Ensures all staff and students have signed an acceptable use agreement form and understand that they must report any concerns;

(c) Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;

(d) Informs users that all computer use including Internet use is monitored;

(e) Informs staff and students that that they must report any failure of the filtering systems directly to the Teacher or Line Manager or IT Services Manager. Our system administrator(s) logs or escalates as appropriate to the Technical service provider as necessary;

(f) Requires pupils to agree that they will adhere to our Acceptable Use Policy each time they log on to a computer which is fully explained and used as part of the teaching programme;

(g) Requires all staff to sign an e-safety / acceptable use agreement form at least annually and keeps a copy on file;

(h) Requires all staff and students to accept the e-Safety/Acceptable Usage Policy online before being able to access the network;

(i) Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school;

(j) Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and CPD sessions and teaching programme;

(k) Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school Behaviour Management Policy;

(l) Ensures the named child protection officer has appropriate training;

(m) Provides advice and information on reporting offensive materials, abuse / bullying etc available for pupils, staff;

(n) Provides e-safety advice for pupils, staff; and

(o) Reserves the right to immediately refer any material we suspect is illegal to the appropriate authorities – Police – and the Local Authority.

9. Education and training:

9.1 Jack Hunt School:

(a) Fosters a ‘No Blame’ environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;

(b) Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or the IT Services Manager.

(c) Ensures pupils and staff know what to do if there is a cyber-bullying incident;

(d) Ensures all pupils know how to report any abuse;

(e) Has a clear, progressive e-safety education programme throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience

(f) Ensures that when copying materials from the internet, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

(g) Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, such as age appropriacy. This will include risks associated with pop-ups; buying on-line; on-line gaming / gambling;

(h) Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection; and

(i) Makes training available annually to staff through CPD.

10. Managing Email

10.1 Jack Hunt School:

(a) Will inform the Police, if necessary, if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

(b) Manages accounts effectively with up to date account details of users.

(c) Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

(d) Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus software, as well as direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

10.2 **Pupils:**

(a) Pupils are introduced to and use e-mail as part of the ICT scheme of work.

(b) Pupils are taught about the safety of using e-mail both in school and at home

(c) Pupils sign the school Acceptable Use Form to say they have read and understood the e-safety rules, including e-mail usage and we explain how any inappropriate use will be dealt with.

(d) Parents agree to the Acceptable Usage Policy online when they apply for a pupil placement at the school.

Staff

10.3 Staff must only use School e-mail systems for professional purposes as described in C16 of the School handbook.

10.4 Access in school to external personal email accounts may be blocked.

10.5 Staff must never use email to transfer staff or pupil personal data. Staff must seek guidance from the IT Services Manager before carrying out any activity of this nature. Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. Such emails should follow the school 'house-style'. Staff must ensure they double check all recipients email addresses are correct before sending and be aware of software features such as auto-fill when entering recipients

10.6 The sending of chain letters is not permitted.

10.7 The embedding of adverts is not allowed.

10.8 All staff sign our Acceptable Usage Policy to say they have read and understood the e-safety rules, including e-mail usage and we explain how any inappropriate use will be dealt with.

11. Managing the Network and Equipment

11.1 Using the school network, equipment and data safely: general guidance:

(a) The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

(b) The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network. Any encryption keys used to encrypt files of any kind are to be registered with the IT Support Department to ensure the school has continued access.

Policy / Procedure:

11.2 To ensure the network is used safely this school:

(a) Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;

(b) Provides staff and students with an individual network log-in username;

(c) Gives all pupils their own unique username and password which gives them access to the Internet, the Learning Platform and their own school approved email account;

(d) Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

(e) Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as security restrictions confidential information would be compromised;

(f) Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

(g) Requires all users to always log off or lock workstations when they have finished working or are leaving the computer unattended;

(h) Requires that where a user finds a logged-on machine, they must always log-off and then log-on again as themselves;

(i) Requests that Staff DO switch the computers off at the end of the day;

(j) Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities;

(k) Maintains equipment to ensure Health and Safety protocol is followed;

(l) Ensures that access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;

(i) e.g. teachers access report writing module; SEN coordinator – SEN data;

(m) Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems;

(n) Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support;

(o) Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;

(p) Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;

(q) Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;

(r) Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the Local Authority's approved secure system.

(s) Follows Local Authority advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;

(t) Ensures that our wireless network has been secured to industry standard Enterprise security level with appropriate standards suitable for educational use;

(u) Ensures all computer equipment is installed professionally and meets health and safety standards;

(v) Ensures that projectors are maintained so that the quality of presentation remains high;

(w) Reviews the school ICT systems regularly with regard to health and safety, performance, robustness and security.

12. Dealing with Infringements

12.1 Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures as appropriate. For Staff the following infringements will be dealt with via the application of the Disciplinary Rules & Discipline Procedures for all Staff Policy:

Misconduct

12.2 Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc;

12.3 Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored;

12.4 Not implementing appropriate safeguarding procedures;

12.5 Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community;

12.6 Misuse of first level data security, e.g. wrongful use of passwords;

12.7 Breaching copyright or license e.g. installing unlicensed software on network;

12.8 Allowing access to unauthorised persons ie family, friends to School equipment which will compromise the security of personal data;

Gross Misconduct

12.9 Serious misuse of, or deliberate damage to, any School computer hardware or software;

12.10 Any deliberate attempt to breach data protection or computer security rules;

12.11 Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

12.12 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;

12.13 Bringing the school name into disrepute.

Use of digital and video images

12.14 Photograph and Video

We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

12.15 Website

The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained, delegated to authorised personnel.

12.16 Learning platform

Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.

Photographs and videos uploaded to school systems will only be accessible by members of the school community.

12.17 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission from SLT or the Headteacher except where disclosed to the Police as part of a criminal investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff without the staff member's permission.

A CCTV Policy exists to supplement information given as an overview in this document.

13. Consent from Parents

13.1 Consent is gained from Parents through the online process of applying to join Jack Hunt School. Unless a parent does not give consent pertaining to their child, the school allows students access to:

(a) the Internet at school

(b) the school's chosen email system

(c) the school's online virtual learning environments

(d) ICT facilities and equipment at the school.

13.2 The school cannot ultimately be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. The school can, if necessary, check a student's computer files and the Internet sites they visit at school and may contact a parent/carer if there are concerns about a student's e-safety.

Students are taught about e-safety and are expected to agree to an Acceptable Use statement regarding their use of the facilities provided to them.

14. Staff Acceptable Use Agreement Policy (AUP)

Staff are expected to read, understand and countersign the Acceptable Use Policy Agreement at least annually. The points of compliance are:

I will only use the school's technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

I will not reveal my password(s) to anyone.

I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it without delay. I will not use anyone else's password if they reveal it to me and will advise them to change it.

I will not allow unauthorised individuals to access any school systems.

I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.

I will not transfer personal data to a device or system unless it has been approved and registered by the IT Support Team (under direction of the IT services Manager).

The use of external storage devices such as (including but not limited to) USB memory sticks, SD cards external hard drives is not allowed, unless approved and registered by the IT Support Team (under direction of the IT services Manager). These devices must be protected by encryption and any encryption keys must be registered with the IT Support Team if used for storing or processing personal data.

I will not engage in any online activity that may compromise my professional responsibilities.

I will only use the Schools email system for school business.

I will use the bcc feature of Outlook when emailing parents or external recipients to ensure their contact details are hidden from each other.

I will only use the school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

I will not browse, download or send material that could be considered offensive.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager or IT Services Manager.

I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

I will not publish or distribute work that is protected by copyright.

I will not connect a computer, laptop or other device to school equipment without authorisation from the IT Services Manager.

I will not use personal equipment for the taking or transferring of images of pupils or staff.

I will use the school's Learning Platform in accordance with school protocols.

I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.

I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I will embed the school's e-safety curriculum into my teaching.

I will alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.

I will only use School systems in accordance with any corporate policies.

I understand that all Internet usage / and network usage is logged and this information could be made available to my manager on request.

I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.

I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

Signature .... Date..

Full Name .... (printed)

Job title ....

15. Version History

15.1 Table of Versions

VERSION	ACTION	RESPONSIBLE	DATE
1.0	Draft policy published	Andy DUFFY	19/02/2016
2.0	Policy reviewed, standard template, parent and student AUP removed (now online)	Andy DUFFY	20/09/2016
2.1	Minor amendments / reconfig and draft put into issue pending SLT and GB approval	Matthew DEERE	12/10/2016
2.1	Resources Management Committee approval to publish given	Matthew DEERE	31/10/2016
2.2	Minor grammatical amendments, changes to job	Andy DUFFY	14/03/2019

	title, additional clarification of use of external media (USB sticks)		
2.2	Approved by Governors at Finance Committee	Matthew DEERE	23/09/2019
2.3	Addition of Lightspeed filtering for mobile devices, bcc for external mail recipients and minor grammatical amendments	Andy Duffy	21/09/2021
2.3	Approved by Governors at Finance Committee	Matthew DEERE	27/09/2021
2.4	Updated as part of annual review, with changes to reflect Code of Conduct updates		