Acceptable Use Policy

September 2022

The requirement to ensure that pupils, staff and, indeed, all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound.

This framework of e-safety, or acceptable use policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

The intention of this evolving policy is:

- To maximise e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use

As such, the school more specifically intends:

1. To provide a secure network for the school and secure means of home/school access
2. To monitor traffic, log incidents and act accordingly
3. To establish key standards and behaviour for e-safety across the school, in-keeping with those of the Local Authority
4. To coordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines and acceptable use policies for pupils, staff, parents and governors
5. To ensure that we adhere to e-safety issues related to new government policies affecting schools
6. To monitor the school's responses to e-safety matters and act accordingly
7. To have a named School Contact (Mr David Heather), to coordinate the development and implementation of e-safety policies, with clear designated responsibilities, and liaise with the Local Authority in such matters

E-safety is a whole-school issue. As such, the whole school has a responsibility to promote it.

Guidelines

The AUP aims to:

- To reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school

and that these responsibilities are not confined to the physical location of the school.

- enable young people to develop their own protection strategies when adult supervision and technological protection are not available;
- provide information on where to seek help and how to report incidents;
- help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online;
- provide guidelines for parents, carers and others on safe practice;
- ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders;
- ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme

Strategy

This policy is the result of ideas discussed by staff, Governors and School Council members. Parents are informed through the home/school agreement which is signed by them and the pupils' AUP which is signed by the children when they begin to use the internet. These are kept in the yellow files in the office. Children are reminded of this agreement regularly and a copy of the pupils' AUP is displayed near the laptop cabinet.

Passwords

Staff and pupil passwords are kept private and only the holder can change them. It is accepted that from time to time, e.g. forgetting a password, the Head, or other designated members of staff, can help to create a new password but s/he will not know what it is. Computers should not be left in 'logged on' mode. It is good practice for users to change their password regularly.

Emails

It is accepted that staff may send emails and attachments to recipients outside the school. Children may only do so under the supervision and direction of their teacher.

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system which is updated regularly. The network is set up to automatically scan laptops and other portable devices every time they are connected to the school system.

Video conferencing

Under the direct supervision of a teacher/TA children may participate in video-conferencing with other schools. The details on protocol around ,for example, Google Meet and virtual teaching during a pandemic, is covered in the safeguarding policy

Inappropriate content and language

The policy provides the following definitions of what is deemed 'inappropriate' for both email and website use.

Inappropriate email content:

abusive	bullying	defamatory
disruptive	Harmful to council, LA or school morale	harassing
insulting	intolerant	obscene
Offensive*	Politically biased**	Sexual innuendo

- *e.g. material that can be construed as offensive on the grounds of gender, race, ethnicity, disability, sexuality, religion, age, size/stature, status.
- **no partiality towards or against any political grouping or individual.

The type of language that is used in emails should be no different to that which is used in face to face situations.

Inappropriate web content:

Adult material	Incitement (e.g. racism)
Chat rooms/instant messaging (except that promoted by the school for educational purposes)	Personal ads. Dating
Downloads of freeware, shareware, evaluation packages (except by	Newsgroups/forums

authorised persons and in compliance with copyright law)	(except that promoted by the school for educational purposes)
Downloads of ring tones, screensavers and games (except any promoted by the school for educational purposes)	Internet peer to peer networks

Staff

The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies and DFE publications such as Keeping Children Safe in Education 2020. Working at this school means acceptance of those policies, including this AUP.

As such:

- Staff must not allow any emails between themselves and pupils to be anything other than school business.
- During ICT pupils should be made aware of the procedures for reporting accidental access to inappropriate materials. In any instance of deliberate misuse the Head must be informed and the pupil will be dealt with in accordance with the school's behaviour policy.
- Staff e-mail accounts may be used for personal use but staff need to be aware that conducting any personal transactions could result in residual information remaining on the hard drive which may be accessible to others. **Neither the school nor the Local Authority can accept any liability for any resulting loss or damage.**
- Staff should log-off whenever they are not using a laptop. **The security of school laptops out of school, lies with the staff. If laptops are taken off school premises, staff must accept responsibility for them.**
- PCs and laptops for pupils must be arranged in classrooms to allow good teacher supervision.
- Staff should avoid using a mobile to discuss sensitive information in public places
- Staff should be aware of the guidance on the use of mobile phones in school in the child protection policy
- Staff should be aware of school policies which cover phone use; viruses; sharing of information etc.
- Staff should be aware of GDPR
- Staff should be aware of 'Contextual Safeguarding' and be alert to any safeguarding issues, particularly those arising from use of social media, peer-on peer abuse using e.g. sexting. Guidelines set out in the child protection policy should be followed.

Pupils

Pupils are involved, through the School Council

- Pupils are not encouraged to bring in to school personally owned devices unless they have been so requested by their teacher. Any such device should be handed into the school office for safekeeping until such time as they are required or collected at the end of the school day.
- The school cannot accept any responsibility for personally owned electronic devices and pupils are requested not to bring them in.
- Google suite should be used as the means of accessing such data off school premises.
- The school accepts the use of school email addresses by pupils to communicate with other pupils, to staff and to pupils in other schools providing they adhere to the pupil AUP.
- Pupils are made aware of the procedures for reporting accidental access to inappropriate materials.

If children accidentally find inappropriate material they are to report it to their teacher who will alert the Head so that he can take steps to rectify this. Staff who find inappropriate material will report it directly to the Head. Children need to be taught this procedure in their ICT lessons. Staff are made aware of their responsibilities in this during staff training and by having their own copy of the policy. Any concerns regarding safeguarding incidents will be referred by the Leadership Team to the Safeguarding Governor as appropriate.

Sanctions

Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school. Violations of the rules may result in a temporary (or permanent) ban on internet use; additional disciplinary action may be taken regarding inappropriate language or behavior; if applicable other authorities may be involved.

This policy will be reviewed annually.

Policy endorsed by the Governing Body on …….

Signed ……Chair of the Governing Body

Equal opportunities

All young people will be treated equally, regardless of race, creed, disability or gender. The policy will be applied regardless of culture, faith or belief.

This policy should be read in conjunction with the ICT policy; Data collection and security policy; The School Continuity Management Policy; The Child Protection policy; Discipline and behaviour; Anti-bullying and harassment policy

Useful websites:

www.thinkuknow.co.uk

www.ceop.police.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Appendix 1

Pulford School Pupil Acceptable Use Agreement

- I will use the school's ICT equipment for schoolwork and homework. If I want to use the school's equipment for anything else I will ask permission first.
- I will only use MY user logins and passwords.
- I will not share my password with anyone. I will tell my teacher if I think someone else knows my password. If I know someone else's password I will not sign on as them.
- I will never give out personal details e.g. photograph, address, full name or telephone number. If I have to use an online name, I will make one up. I will be aware of stranger danger when I am communicating on-line.
- I will never arrange to meet someone I have only previously met online. It could be dangerous.
- I will only use the internet with an adult present.
- I will make sure that all my communication is responsible, polite and appropriate.

- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I see anything that makes me feel uncomfortable, I will always tell an adult.

- I will only look at or delete my own files.

- I will ask for permission before opening an email or an attachment from someone I do not know.

- I will only download software, pictures etc with an adult's permission.

- I understand that I must not bring software or disks into school without permission. Also that any I do bring in need to be scanned for viruses before opening.

- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.

- The school may check my files, emails etc. and the Internet sites I visit.

- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

- I have read and agree to these guidelines

  Signed……. Date……