Eskdale School

A place of belonging, a place of inspiration

ICT Acceptable Use Policy

Eskdale School aims:

To develop as a vibrant, dynamic community committed to the principles of "Every Child Matters" so that all of our students

- are safe and healthy
- enjoy and achieve
- make a positive contribution
- experience success so that they are equipped to make their way in the world of work**.**

Document Status	
Date of Policy Adoption by Governing Body: January 2006	
Reviewed	June 2018
Next Review	June 2021
Signed (Chair of Governors)	

ICT Acceptable Use Policy

In order to maintain a working ICT network that our users can use safely, Eskdale School imposes certain regulations on the use of its computers.

1. Users must not download or install any computer software that does not have prior approval by the school e.g. games, screensavers etc.
2. Users must not download, create or transmit material which is designed or likely to cause annoyance, inconvenience or upset;
3. Users must not create or transmit any defamatory material;
4. Users must not transmit any material which infringes copyright regulations;
5. Users must not transmit unsolicited commercial or advertising material;
6. Users must not deliberately attempt unauthorised access to facilities or services accessible by Eskdale School; This includes, but is not limited to;
   - Wasting staff effort or networked resources;
   - Corrupting or destroying other users' data;
   - Violating the privacy of other users;
   - Disrupting the work of others;
   - Using the Schools computer systems and Internet connection in a way that denies service to others;
   - Continuing to use an item of networking software or hardware after the school has requested that use ceases;
   - Other misuse of the school's computer systems or networked resources, such as the introduction of 'viruses';
7. Users must not register on any website, chat room or newsgroup in the name of Eskdale School;
8. Internet/email/Network use may be monitored to ensure compliance with the above;
9. Individual passwords must **never** be shared or revealed to anyone. To do so makes the authorised user liable for the actions the other party takes while using that password.
10. Users must never send emails or attachments, or store emails or attachments that are defamatory, abusive, obscene, indecent, racist, sexist, in breach of copyright or otherwise inappropriate
11. Users should exercise due caution in revealing any personal details to email or Internet enquiries
12. Users should work offline whenever possible to avoid overloading the computer systems
13. Internet access is continuously logged and monitored on a regular basis.
14. Internet access is filtered by Eskdale School and North Yorkshire County Council Schools Services in line with Department for Education recommendations.

If any of the above conditions are disregarded, the school reserves the right to reduce or withdraw access to the Internet and /or Computer Systems.

Student/Parent Declaration

Both the student and, if applicable, the parent or guardian must sign this document before a user account will be issued to the student.

Please read carefully before signing

To be completed by the student:

As a school user of ICT, I HAVE READ AND AGREE TO COMPLY with the school policy on its use. I will use the network in a responsible way and observe all the restrictions as explained herein.

Student signature…… Date……

Print Name: ……

If applicable, Form …… Year Group ……

To be completed by the Parent or Guardian (unless an adult student):

I have read and understand the School rules for responsible ICT Use, and as the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the Internet, e-mail and other ICT facilities at school. I understand that the school will take reasonable precautions to ensure that students cannot access inappropriate materials, but accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet. I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.

Parent/Guardian signature…… Date……

Print Name: ……

Data Protection Update for new GDPR legislation.

Dear All,

This is a good time for a reminder about data security. We are all responsible for protecting the data in school whether paper or electronic. Personal and sensitive is anything which may identify additional information about a child.
Most staff members will be involved with various pieces of data regarding students.
Data regarding dates of birth, pupil premium, SEND designation, achievement are all considered personal and sensitive.

- Paper records - These must be shredded, or put in the bag in the office. SEND and medical notes must be stored securely and not left on your desk.
- Emails - Any of this information sent electronically must be password protected – see the staff room notice board for the password.
- Electronic data - All data on memory sticks if it leaves the building must be on an encrypted stick.

Other things to think about and remember;

- Your computer – it must not be left unlocked when you are not in the room.
- SIMS – classlists – if you project them, they must not display sensitive information. If you are writing up a behaviour event – can all the class see what you are writing?
- Secure staff areas are on common – staff only or staff only reporting. Photos should be stored in staff only.
- Phones – school mobiles are available for trips, and school cameras are available. Your personal mobile should not be used for any photo. Do not give out your phone number for trips.
- Learning Gateway – if you access this at home do you log out after use? Does your computer remember your password? Who else could see that information?
- Phone numbers – some are not freely available and so what about messages to phone someone – think where you leave this.
- Meetings with parents – where do you record this? If it's in a book, where do you leave this?
- The staffroom has confidential information and is locked at the end of the day and at the weekend – if you use the staffroom outside these hours, make sure you leave it secure.
- We do have outside users in school during the evenings and weekends – do not assume they stay in one place, they may roam around and if they came into your room could they get access to personal and sensitive data?

Acceptable Use Agreement
ICT and E Technology

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT and the related technologies such as email, the internet, web2 technologies and mobile devices. Members of staff should consult with the Headteacher for further information and clarification.

Members of staff:

- Must only use the school's email, internet and intranet and other related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body. Individual employees' internet and other related technologies can be monitored and logged and can be made available, on request, to their line manager or Headteacher.
- Must only use approved, secure email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Should not use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher; they should only used for professional purposes.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher.
- Should ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, misused.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Twitter, Instagram does not question or bring their professional role into disrepute. Members of staff:
  - Are advised to consider, and set appropriately, their privacy settings on such sites.
  - Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
  - Should not communicate with pupils, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.

User Signature

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in line with the School's Disciplinary Procedure. I have read the guidelines for staff and will adhere to them.

Signature …… Date ……..

Full Name (Printed) …… Job Title ……