

Scramerston First School

ICT Acceptable Use Policy

Staff and Volunteers

As a professional organisation with responsibility for children's safeguarding it is important that all staff and volunteers take all possible and necessary measures to protect data and information systems from infection, unauthorized access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy. All members of staff and volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

The aims of this Acceptable Use Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.
- To give pupils clear guidance on safe and acceptable use of these resources.
- To ensure that children, staff, parents, governors and volunteers are aware of the expectations of acceptable use when using electronic devices and the internet in school and at home.

The AUP will be revised annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

General

- All children, staff and adults who visit the school regularly will be expected to sign the AUP.
- Internet sessions will always be supervised by a teacher.
- Filtering systems are used by our Internet Service Provider, (Northumberland County Council), in order to minimise the risk of exposure to inappropriate material.
- Northumberland County Council will monitor Internet usage. The summary of this will then be reviewed by the head teacher, Helen Harrison and the e-safety officer, Emma Holleywell.
- Students and teachers will be provided with continuous training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software is present on all lap-tops and net-books and is updated and checked automatically on a daily basis.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

- Staff and volunteers will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Staff and volunteers will report accidental accessing of inappropriate materials in accordance with school procedures.
- Staff and volunteers will use the Internet for educational purposes only.
- Staff and volunteers will **NEVER** disclose or publicise personal information.

- Staff and volunteers will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or management reasons.

Email

- Staff will use approved email accounts in school.
- Staff and volunteers will not send or receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.

Internet Chat/ Blogging/ Forums

- These mediums may only be accessed by children under direct instruction from a member of staff.
- Communication via these mediums will be monitored by the class teacher.
- Blogging/ chat may only take place via the county VTLE.

Personal Devices

- Children are prohibited from bringing personal devices into school.
- Staff personal devices may only be used in the staffroom.

Support Structures

Staff and volunteers will be made aware of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings and withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

***For additional information and guidance please refer to the e-safety policy.**

I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used with parental permissions.

I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

I will report all incidents of concern regarding children's online safety to the Named Person and/or the e-Safety Coordinator (E.Holleywell) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator.

My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the staff and volunteer acceptable use policy.

Signed _____

Date _____