



**Our moral obligation is to help our children become successful learners, confident individuals and responsible citizens, and we believe that this policy, will help us achieve this goal.**

## **Acceptable Use Policy - EYFS and Key Stage 1**

### **1 Preface**

This document sets out Barnham Primary School's Acceptable Use Policy. There are adaptations of the policy for the various Key Stages.

Access to the school IT network and the school 'cloud services' is a privilege for all users and should not be regarded as an automatic right. All users must follow the conditions described in this policy when using the school network, and school cloud services.

For pupils, teachers will show them how to safely use the resources available through the IT systems. Staff and other users can receive advice from the school IT manager.

School staff will regularly check the network to make sure that it is being used responsibly by all.

The school will not be responsible for any loss of data or work as a result of the system or user mistakes in using the system.

The use of any information gathered via the network and the school internet connection is at the user's own risk.

This Acceptable Use Policy also includes the use of any other IT devices, mobile phones and cameras and including any social media forms and network sites, where any direct or indirect reference is made regarding the School, pupils or staff or work related matters.

Users that do not follow adhere to the policy may face the following sanctions:

- Close monitoring of their school network activity,
- Detailed investigation of their past school network activity,
- Withdrawal of network access privileges
- Behaviour investigation of pupils
- Disciplinary investigation of staff
- In some cases, criminal prosecution.

### **Acceptable Use Policy (AUP)**

The networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any expression of a personal view about the school or Trust matters in any electronic form of communication must be endorsed to that effect.





Any use of the network that would bring the name of the school or the Trust into disrepute is not allowed.

The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Independent pupil use of the internet or the school's network will only be permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

### **Our overarching Network etiquette and privacy rules.**

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

Use appropriate language – users should remember that they are representatives of the school on a global public system.

Illegal activities of any kind are strictly forbidden.

Do not use language that could be seen as bullying, discriminatory or calculated to incite hatred against any person or group of persons, including ethnicity, religion or other person or group with a protected characteristic.

Privacy – do not reveal any personal information (for example date of birth, home address, telephone number) about yourself or other users.

Do not trespass into other users' files or folders.

Password – do not reveal your password to anyone. If you think someone has learned your password then contact member of staff responsible.

Electronic mail is not guaranteed to be private.

Messages relating to or in support of illegal activities will be reported to the authorities.

Do not send anonymous messages.

Disruptions – do not use the network in any way that would disrupt use of the network by others.

Users will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

Users finding unsuitable websites through the school network should report the web address to the school IT manager.





Do not introduce any USB drives, data disc or other portable devices into the network without having them checked for viruses.

Do not use personal devices to transfer data or pictures of a non-educational nature onto the school IT system.

Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity.

Downloading some material is illegal and the police or other authorities may be called to investigate such use.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.

Files held on the school's network will be regularly checked by the member of staff responsible.

It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet or intranet does not occur.

## **2 Pupil Acceptable Use Policy EYFS and Key Stage 1**

All pupils at Barnham Primary School must follow the rules in this policy when using school computers, and the school cloud services.

Pupils that do not follow these rules may find:

- They are not allowed to use the computers.
- They can only use the computers if they are more closely watched.

Their teachers and school staff will show pupils how to use the computers, help them understand the rules and will supervise their use of the computers.

### **2.1 Computer Rules**

- 1 Pupils will only use polite language when using the computers.
- 2 Pupils must not write anything that might upset someone or give the school a bad name.
- 3 Teaching or support staff will regularly check pupils' work on the school computers.
- 4 If a Teacher thinks a pupil has been breaking the rules they will check on how that pupil has used computers before.





- 5 Pupils must not tell anyone their name, address, or my telephone number over the Internet.
- 6 Pupils must not share their username and passwords with anyone else but their parents.
- 7 Pupils must never use other people's usernames and passwords or computers left logged in by them.
- 8 Pupils will tell their Teacher if they think someone else has their password.
- 9 Pupils must log off once they have finished working on a computer.
- 10 Pupils must not use the computers in any way that stops other people using them.
- 11 Pupils will report to their Teacher any websites that make them feel uncomfortable.
- 12 Pupils will tell their teacher or a member of staff straight away if they receive any messages that make them feel uncomfortable.
- 13 Pupils will not harm any IT equipment or the work of another person on a computer.
- 14 Pupils must tell a teacher straight away if they see something that they think they should not see and will not show it to other pupils.

## **2.2 Unacceptable Use**

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Wasting time or resources on school computers.

The use of camera, audio and/or video recordings on pupils' own devices or school devices is prohibited whilst in School unless this has been approved by the Head Teacher. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.

## **3 Network Security**

If pupils discover a security problem, for example being able to see other pupil's work areas, they must inform a member of staff who will inform the ICT Manager. Pupils identified as persistently failing to adhere to this policy will not be allowed to access the network.

## **Services**





There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

Cloud services are dependent on servers, connections and equipment which are outside of the control of the school. The availability of these systems, and any errors, data loss or corruption that may occur through the use of these systems, are the responsibility of the service providers and are subject to their standard terms of use. Users are reminded that data stored on Cloud services is not backed up by the school and recovery options will be limited in the event of accidental deletion or corruption of such data.

