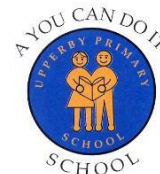




# Upperby Primary School

## Online Safety Policy



### Introduction

At Upperby Primary School we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

### The Law

Our Online Policy has been written by the school, using advice from Cumbria LSCB and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Computing, Safeguarding and Data Protection policies. As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at [www.education.gov.uk/schools](http://www.education.gov.uk/schools).

### Roles and Responsibilities

**The Headteacher, alongside the Designated Safeguarding Lead (Paula Burns) will:**

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

**Teachers and Staff will:**

- Keep passwords private and only use their own login details, which are stored securely
- Monitor and supervise pupils' internet usage and use of other IT resources
- Adhere to the Acceptable Use Agreement
- Promote e-safety and teach e-safety units as part of computing curriculum
- Engage in e-safety training
- Only download attachments/material onto the school system if they are from a trusted source

- When capturing images, videos or sound clips of children, only use school cameras or recording devices

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

#### **Governors will:**

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of online-safety in school

#### **Teaching and Learning**

The school will actively teach online safety at an age-appropriate level. The school follows a scheme of work for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics (Be Internet Legends). Online safety will also be embedded throughout learning whenever children are using ICT in other lessons such as KidSafe sessions.

#### **Monitoring safe and secure systems**

Internet access is regulated by Cumbria County Council supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. saved to cloud programs such as CPOMS. If personal data has to be saved to a data block, these are encrypted.

#### **Safe use of the Internet and Web Filtering**

- \* All staff and pupils will have access to the internet through the school's network
- \* All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- \* All children must read and sign the Pupil Acceptable Use Agreement.
- \* If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher / DSL.
- \* If an adult finds a site that they consider unsuitable they should report it to the Headteacher

#### **The use of Email**

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails. All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email.

### **The school website**

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

### **Social Networking, Social Media and Personal Publishing**

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, such as Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home, but will be reminded that there are clear age restrictions.

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

### **The Use of Cameras, Video and Audio Recording Equipment**

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the agreed school systems such as Twitter and the school website, when permissions have been sought from parents. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

### **Personal mobile phones and mobile devices**

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include toilets and changing areas, including where children change for swimming.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

### **Management of online safety incidents**

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

### **Working in Partnership with Parents**

Parents' attention will be drawn to the online safety policy through the school newsletters, information evenings and on the school website. A partnership approach with parents will be encouraged. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement on entry to the school (as of September 2019).

### **Protecting School Staff**

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

### **Safeguarding – scope of this policy**

(See also Safeguarding and behaviour policies)

The Education and Inspections Act 2006 empowers the Head Teacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents /carers of incidents of inappropriate e-safety behaviour that take place out of school.

### **Monitoring and Reviewing the Policy**

This policy is monitored on a day-to-day basis by the head teacher, who reports to governors about the effectiveness of the policy on request. The Policy is the governors' responsibility and they review its effectiveness every two years. They do this by discussion with the head teacher.

This policy was agreed by the governing body on 19<sup>th</sup> December 2018 and was updated by the governing body on 18<sup>th</sup> November 2020. Date of review November 2022.

## ICT Pupil Acceptable Use Agreement and Online Safety Rules

- I will log on using my own username and password.
- I will tell an adult straight away if something on the computer has upset me or worried me so if I find anything or anyone online that makes me feel uncomfortable, unsafe or uneasy in any way, I will **tell an adult** immediately.
- I will be polite and friendly to everyone I speak to on the computer so I will make sure that all online contact with other children and adults is **responsible, polite** and **sensible**.
- I will only send pictures, videos or words that are kind and friendly so I will only upload or add images, video, sounds or text that are **appropriate, kind** and **truthful** and will not possibly upset someone.
- I will keep my personal details **private** when I'm online.
- I will be sensible on the computer and the internet and they will speak to my parents and carers if I am not.
- for the way I behave online, and I know that these rules are to keep me safe.

**Think before you click!**

### **Dear Parent/ Carer**

ICT, including the internet, email, digital and mobile technologies has become an important part of learning in our school. We expect all children to act safely and be responsible when using any ICT. Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your class teacher.