Flintham Primary School

E-Safety and Acceptable Use of Policy

June 2022

'Inspiring A Love Of Learning'

Our School Vision is

We aspire to provide everyone with…

- **an excellent holistic education through an inspiring, creative and ever evolving curriculum.**
- **an understanding that there is no limit to their potential.**
- **the foundations to face the various challenges of life and be respectful, responsible and caring citizens making a positive contribution to their community and wider society.**
- **a love of learning which continues to develop enquiring minds and enrich their lives.**

FLINTHAM PRIMARY SCHOOL
SUPER SIX AIMS

Flintham Primary School

E-Safety and Acceptable Use Policy

1. URGENT CONCERNS

If you have an immediate E-Safety concern, please report it to the Head Teacher or member of the SLT. This may be done orally in the first instance to ensure speed of response but should be backed up by recording the incident using the Incident report form (available in the E-Safety folder) at the earliest opportunity.

2. Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include: Websites, Learning Platforms and Virtual Learning Environments, Email and Instant Messaging, Chat Rooms and Social Networking, Blogs and Wikis, Podcasting, Video Broadcasting, Music Downloading, Gaming, Mobile/Smart phones with text, video and/or web functionality, other mobile devices with web functionality. Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Flintham Primary School, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This E-Safety and Acceptable Use Agreement is inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, ipads, whiteboards, digital video equipment, etc.)
Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.

3. Roles and Responsibilities

Governors are responsible for:

the approval of this policy and reviewing its effectiveness.

The Headteacher is responsible for:

- ensuring that everyone in school - including staff, volunteers and pupils - knows how to stay safe, including on-line.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- ensuring that staff receive suitable training and development to enable them to carry out their role.
- ensuring that e-safety issues that occur within school and outside of school are appropriately dealt with, liaising with the Local Authority Designated Officer (LADO) or police as appropriate.
- Providing information to the Governing Body, as appropriate.

Lead Teacher for Computing and E-safety is responsible for:

- ensuring staff have an up-to-date awareness of e-safety matters.
- updating school e-safety policy and curriculum content, as appropriate.
- monitoring curriculum delivery and outcomes.
- liaising with the Headteacher to provide training and advice to staff.

Classroom staff are responsible for:

- maintaining an up-to-date awareness of e-safety matters and of school e-safety policy and practice.
- ensuring they have read and understood the appropriate computing agreements.
- reporting any suspected misuse or problem to a member of SLT and report on CPOMS.
- ensuring digital communications with pupils are only on a professional level and carried out using official school systems, ensuring multiple recipients are blind copied into emails so personal data is not shared with others.
- understanding that social media can play an important part in communication between the school and parents/carers; but knowing it must be used in an appropriate and safe way.
- informing the Headteacher before setting up a digital resource such as a student blog space.
- ensuring that appropriate steps are taken to make such platforms 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from users/contributors.
- teaching agreed e-safety objectives, as outlined within the Computing and PSHE curriculum.
- ensuring that children understand and follow the school's 'Acceptable Use' policy.
- making sure that children are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that children understand school policy in relation to mobile phones on site.
- ensuring that internet use in lessons is pre-planned and children are guided to sites that are checked as suitable for their use.

Children (appropriate to age / stage of pupil):

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Computing/E-Safety Policy covers their actions outside of the school gates and at home.

Parents

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of technology than their children. The school will therefore take every opportunity to help parents understand these issues through communications and the website.

Designated Persons for Safeguarding should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

4. Managing the school E-Safety messages

We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used. We teach e-safety at the beginning of every half term and through certain topics in our PSHE lessons. The e-safety policy will be introduced to the pupils at the start of each school year. E-safety posters will be prominently displayed.

E-Safety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about E-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher, trusted staff member.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum in Year 3, 4, 5 & 6.

5. Password Security

All users are made aware of the Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy. Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. If you think your password may have been compromised or someone else has become aware of your password report this to the E-Safety co-ordinator or head teacher. Staff are aware of their individual responsibilities to protect the security and confidentiality of school network and assessment portal, including ensuring that passwords are not shared or stored elsewhere, are strong passwords which are changed periodically.

-Data Security
The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not:

- take copies of the data
- allow others to view the data
- edit the data unless specifically requested to do so by the head teacher and/or governing body.

6. Managing the Internet
The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. The use of the internet is monitored and internet filters are in place to ensure pupils are only accessing content that is appropriate to them. Whenever any inappropriate use is detected, it will be followed up.

The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- Staff will preview any recommended sites before use.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure
School internet access is controlled through the LA's web filtering service. This system ensure high levels of filtering for all users to prevent access to inappropriate content, including material relating to terrorism and extremism.

- Flintham Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998 Section 29 of the Counter-Terrorism and Security Act 2015. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the teacher and then to the e-safety co-ordinator. It is the responsibility of the school, by delegation to Nottingham's ATOM services, to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor the network managers to install or maintain virus protection on personal systems.
- Pupils are not permitted to download programs or files on school-based technologies.
- If there are any issues related to viruses or anti-virus software, the e-Safety co-ordinator should be informed.

7. Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under exceptional circumstances the school allows a member of staff to contact a pupil or parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. No image or sound recordings should be made on these devices of any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Mobile telephone should not be used in the classrooms during the school day. Mobile telephone calls, short message services, etc. must never occur in the classrooms during contact time. The office staff will take emergency phone messages should they arise. Staff will only be called to the telephone during contact time in the case of an emergency. Personal devices can be used in the staffroom or offices during staff breaks.

School provided Mobile devices (including phones)

Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used. Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

8. Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good "netiquette".

The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business; personal email addresses should not be used.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses. Email sent to an external organisation should be written carefully before sending. Staff sending emails to parents or pupils are advised to cc. the headteacher, Key Stage Coordinator or Office and send using scholarpack. If staff are sending an email to multiple recipients they should use blind copy so as not to share personal information.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not

revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.

9. Safe Use of Images

Taking of Images and Film-Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Publishing pupils' images and work.
On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways: on the school's internet pages, in the school prospectus and other printed publications that the school may produce for promotional purposes, in display material that may be used in external areas, i.e. exhibition promoting the school general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically). This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.
Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

10. Storage of Images

- Images/films of children are stored on the shared area on the school's secure One Drive.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB
- sticks) without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching and support staff within the confines of the school network.

-Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school will only ever used for specific learning purposes and never using images of children or adults.

-Video Conferencing
Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school. All pupils are supervised by a member of staff when video conferencing. Approval from the Head Teacher is sought prior to all video conferences within school. The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences. No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

11. Safe and Responsible Use of Social Networking Internet Sites

Social Networking sites have dominated the internet and are used by a wide range of users worldwide. Whilst these sites are not appropriate for pupils in the Primary age phase and thereby are not permitted in school, staff should ensure that if they are using sites of this nature or any other associated forums, that under no circumstances should work-related matters be discussed. This is to ensure that people are protected and to minimise the risk of breaching confidentiality and preventing cyber bullying amongst adults. Although the school supports the right for staff to have a private life, caution should be taken when liaising with any person who is connected with the school. On Social Networking sites, where 'friend' requests can be sent and received (e.g. Facebook), staff members should not add any past or present pupils to their Facebook or other Social Network site personal page. Any 'friend' requests from children should be ignored and this should be brought to the attention of the Head Teacher who will alert the parents/carers. Caution should also be used when 'friending' parents and carers on Social Network sites, irrespective of friendships offline.

During conversations or wall posts or any other means of communication on Social Network sites, staff should not mention anything that may bring the school or the profession into disrepute. The school will apply the necessary disciplinary procedures to any breach of this policy.

13. Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the head teacher. Incidents should be logged and followed up.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety co-ordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the head teacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offence.

14. Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

15. Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to the school E-Safety policy by letter and by reporting unsuitable sites etc. to the E-Safety co-ordinator.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).

- The school disseminates information to parents relating to E-Safety where appropriate in the form of website postings and newsletter items.

16. Writing and Reviewing this Policy

Review Procedure

- There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them.
- This policy will be reviewed annually, and consideration given to the implications for future whole school development planning and new/emerging technologies.

Acceptable Use Agreement/Code of Conduct - Staff

Flintham Primary School Acceptable Use Agreement/Code of Conduct: Staff and Governors.

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head teacher, depending on the seriousness of the offence; investigation by the head teacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed reasonable by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details such as mobile phone number and personal email address to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Scholar pack and CPOMs) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional
- role into disrepute.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

The Flintham Primary School Technology Promise

When using technology in school we will:

- ✓ TAKE CARE - when carrying equipment.
- ✓ ASK - before going online.
- ✓ TELL - an adult if something goes wrong or upsets me.
- ✓ THINK - before I click.

We understand that if we are not behaving correctly, we may not be allowed to use technology in school.

All of the children in class ____ agree to this.

Signed by the teacher: _____

The Flintham Primary School Technology Promise

When using technology in school we will:

- ✓ TAKE CARE - when carrying equipment in the classroom and around school.
- ✓ ASK - an adult before going online.
- ✓ SPEAK- kindly to others when sending e-mails and blogging.
- ✓ KEEP- my personal information private (such as password, full name, address and school name).
- ✓ TELL - an adult if something upsets me while I am online.
- ✓ THINK - before I click (especially when printing and deleting).

We understand that if we are not behaving correctly, we may not be allowed to use technology in school.

All of the children in class ____ agree to this.

Signed by the teacher: _____