



Althorpe and Keadby Primary School

Online Safety Policy

Approved by: Althorpe and Keadby Primary School Governing Board

Date approved: May 2022 **Review Date:** December 2024

Reviewed By: Nicola Whitehouse

Contents

Online Safety Policy Content

1. Policy Aims
2. Links with other policies and practices
3. Roles and responsibilities
4. Education and Engagement approaches
5. Reducing Online Risks
6. Safer Use of Technology
7. Google, Scholarpack and Seesaw
8. Social Media
9. Mobile Technology
10. Responding to Online Safety Incidents and Concerns
11. Concerns about learner online behaviour and/or welfare
12. Procedures for responding to specific online concerns

Appendices

Appendix 1: Acceptable Use Agreement for Staff

Appendix 2: Primary Pupil Acceptable Use

1. Policy aims

- This online safety policy takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2019, '[Early Years and Foundation Stage](#) 2017 and '[Working Together to Safeguard Children](#)' 2018.
- The purpose of the online safety policy is to
 - o safeguard and promote the welfare of all members of Althorpe and Keadby Primary School's community online.
 - o identify approaches to educate and raise awareness of online safety throughout our community.
 - o enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - o identify clear procedures to follow when responding to online safety concerns.
- Althorpe and Keadby Primary identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas of risk.
 - o **Content:** being exposed to illegal, inappropriate or harmful material
 - o **Contact:** being subjected to harmful online interaction with other users
 - o **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
 - o Anti-bullying policy
 - o Behaviour policy
 - o Child protection policy
 - o Confidentiality policy
 - o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (*Sarah Tate - Headteacher*) is recognised as holding overall lead responsibility for online safety.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of *Althorpe and Keadby's* school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support (**Code Green**) to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety via CPOMs.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole *school* approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners safe online.

- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and *school* policies and procedures.
- Report online safety concerns via CPOMS, tagging in the relevant people.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the governor with a lead responsibility for safeguarding and/or online safety.
- Ensure that a regular review of the IT filter and monitoring system is effective.

Update with school/community language variations.

It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read, sign and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.

- Identify online safety concerns and take appropriate action by following the *school* safeguarding policies and procedures (CPOMs)
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and *Althorpe and Keadby Primary School* leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age/ability appropriate online safety education - linked to the Education for a Connected World Framework.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

It is the responsibility of parents and carers to:

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from school or other appropriate agencies, if they or their child encounter online issues.
- Use our systems and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

4. Education and engagement approaches

Education and engagement with learners

- The setting will establish and embed a whole *school* culture and will raise awareness and promote safe and responsible internet use amongst learners by:
 - o ensuring our curriculum and whole *school* approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework](#)' and DfE '[Teaching online safety in school](#)' guidance.
 - o ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
 - o reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
 - o implementing appropriate peer education approaches.
 - o creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
 - o involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.

- o making informed decisions to ensure that any educational resources used are appropriate for our learners.
 - o using external visitors, where appropriate, to complement and support our internal online safety education approaches.
 - o providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
- Althorpe and Keadby Primary will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
 - o displaying acceptable use posters in all rooms with internet access.
 - o informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
 - o seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Althorpe and Keadby Primary will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
 - o ensuring age appropriate education regarding safe and responsible use precedes internet access.
 - o teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
 - o educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
 - o enabling them to understand what acceptable and unacceptable online behaviour looks like.
 - o preparing them to identify possible online risks and make informed decisions about how to act and respond.
 - o ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Learners

- We recognise that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- We will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- We will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.
 - o media can have an impact on their professional role and reputation.
 - o highlight useful educational resources and tools which staff could use with learners.
 - o ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

5. Reducing Online Risks

- We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will o regularly review the methods used to identify, assess and minimise online risks.
 - o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in school is permitted.
 - o ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
 - o recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of

not posting any content, comments, images or videos which could cause harm, distress or offence.

6. Safer use of technology

Managing internet access

- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

Filtering and monitoring

- Althorpe and Keadby, governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Appropriate filtering

- Althorpe and Keadby's education broadband connectivity is provided through Schools Broadband.
- Althorpe and Keadby uses **Netsweeper** Netsweeper blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm,

eating disorder and/or suicide content, pornographic content and violent material.

- o Netsweeper is a member of [Internet Watch Foundation](#) (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
 - o Netsweeper integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with Code Green to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to turn off monitor/screen and report the concern immediately to a member of staff who will add to CPOMs and report the URL of the site to technical staff/services.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- If a concern is identified via monitoring approaches we will log via CPOMs and speak to the Safeguarding lead.

Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
 - o Virus protection being updated regularly.
 - o Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - o Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.

- o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- o Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- o Checking files held on our network, as required and when deemed necessary by leadership staff.
- o All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

Managing the safety of our website - <https://www.akprimary.co.uk>

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing images and videos online

- Parents sign permission yearly to allow photographs of their children to be published either on the website / social media and newspapers. All staff are aware of who these children are and recognise the importance of adhering to this.

Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.

- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell DSL lead if they receive offensive communication, and this will be recorded in our safeguarding files/records.

7. Google, Scholarpack and Seesaw

a) Google

- All teaching and support staff have a google account name@akprimary.co.uk. They have appropriate access to our school google drive and calendar.
- We ensure that the use of this is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- Google Privacy and Security Statement: All Google products are continuously protected by one of the world's most advanced security infrastructures, and we vigorously resist any unlawful attempt to access our customers' data. This built-in security automatically detects and prevents online threats, so you can be confident your private information is safe. Google encrypts data at rest by default. We protect this data with multiple layers of security, including leading encryption technology like HTTPS and Transport Layer Security. Google's [data centers](#) use custom hardware running a custom hardened operating system and file system. Each of these systems has been optimised for security and performance. Because Google controls the entire hardware stack, we are able to quickly respond to any threats or weaknesses that may emerge. We are fully committed to the security and privacy of your data and protecting you and your school from attempts to compromise it.

b) Scholarpack

- We use Scholarpack to track learners' progress from the Early Years Foundation Stage up to year 6.
- We ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
 - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
 - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
 - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
 - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

c) Seesaw

April 2020 - In response to the need for home-schooling and to build parent partnerships, all children from years R-6 now have a seesaw account. Seesaw is a platform for student engagement. Teachers can empower students to create, reflect, share, and collaborate. Students "show what they know" using photos, videos, drawings, text, PDFs, and links. It's simple to get student work in one place and share with families, and nothing is shared without teacher

approval. The Early Years Foundation Stage use Seesaw to log observations of children and create a portfolio of their learning journey.

All parents have been consulted about this and log in details shared safely.

- Seesaw complies with the European Union General Data Protection Regulation (the “GDPR”) and makes it easy for EU individuals to exercise their rights described in that regulation. The purposes for which Seesaw collects information, the categories and specific types of information, and their practices and policies regarding the processing of information are described in their Privacy Policy and Data processing agreement on their website.

8. Social Media

Expectations

- The expectations’ regarding safe and responsible use of social media applies to all members of the Althorpe & Keadby community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of the school community are expected to engage in social media in a positive and responsible manner.
 - o All members of our school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- Concerns regarding the online conduct of any member of our school community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff personal use of social media

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our acceptable use of technology policy.

-

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
- o Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
 - All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:
 - o Setting appropriate privacy levels on their personal accounts/sites.
 - o Being aware of the implications of using location sharing services.
 - o Opting out of public listings on social networking sites.
 - o Logging out of accounts after use.
 - o Using strong passwords.
 - o Ensuring staff do not represent their personal views as being that of the setting.
 - Members of staff are encouraged not to identify themselves as employees of school on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
 - All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies, and the wider professional and legal framework.
 - Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
 - Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.

- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the headteacher .
 - o Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL and logged on CPOMs.

Official use of social media

- Althorpe and Keadby's official social media channels are:
 - o Twitter
- The official use of social media sites by Althorpe and Keadby only takes place with clear educational or community engagement objectives and with specific intended outcomes.
 - o The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
 - o Staff use setting provided email addresses to register for and manage official social media channels.
 - o Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.
 - o Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

-

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - o Be aware they are an ambassador for the setting.
 - o Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - o Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - o Ensure appropriate consent has been given before sharing images on the official social media channel.
 - o Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - o Not engage with any private/direct messaging with current or past learners or parents/carers.
 - o Inform their line manager, the DSL of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - o All members of the school community are advised to take steps to protect their mobile phones or personal devices from loss, theft or

damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

- o All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.
- All members of the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, data security and acceptable use of technology.
- Staff will be advised to
 - o keep mobile phones and personal devices in a safe and secure place during lesson time.
 - o keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - o ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
 - o not use personal devices during teaching periods, unless written permission has been given by the headteacher such as in emergency circumstances.
 - o ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

-
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.

- o Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and headteacher.
- Staff will not use personal devices or mobile phones:
 - o to take photos or videos of learners and will only use work-provided equipment for this purpose.
 - o directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

10. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
 - o Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

11. Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the headteacher, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy.
- Welfare support will be offered to staff as appropriate.

Concerns about parent/carers online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL (or deputy). The headteacher

and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.

- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

12. Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children

- The DSL and appropriate members of staff have accessed and understood the DfE “[Sexual violence and sexual harassment between children in schools and colleges](#)” (2018) guidance and part 5 of ‘[Keeping children safe in education](#)’ 2019.
 - o Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- We recognise that sexual violence and sexual harassment between children can take place online. Examples may include;
 - o Non-consensual sharing of sexual images and videos
 - o Sexualised online bullying
 - o Online coercion and threats
 - o ‘Upskirting’, which typically involves taking a picture under a person’s clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
 - o Unwanted sexual comments and messages on social media
 - o Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
 - o immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

- o if content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
- o provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- o implement appropriate sanctions in accordance with our behaviour policy.
- o inform parents and carers, if appropriate, about the incident and how it is being managed.
- o If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
- o if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
 - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
- o review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Althorpe and Keadby Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Althorpe and Keadby will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

Youth produced sexual imagery (“sexting”)

- School recognises youth produced sexual imagery (also known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and the local [KSCMP](#) guidance: “Responding to youth produced sexual imagery”
 - o Youth produced sexual imagery or ‘sexting’ is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
 - o It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
 - o view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
 - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
 - o send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- o act in accordance with our child protection policies and the relevant local procedures.
- o ensure the DSL (or deputy) responds in line with the [UKCIS](#) and KSCMP guidance.
- o Store any devices containing potential youth produced sexual imagery securely
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- o carry out a risk assessment in line with the [UKCIS](#) and KSCMP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
- o inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- o make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the [UKCIS](#) and KSCMP guidance.
- o provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- o implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- o consider the deletion of images in accordance with the [UKCIS](#) guidance.
 - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- o review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Althorpe and Keadby recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.
- Althorpe and Keadby will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
 - o act in accordance with our child protection policies and the relevant KSCMP procedures.
 - o store any devices containing evidence securely.
 - If content is contained on learners personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content. o if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
 - o carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
 - o inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
 - o provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

- o review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - o Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP:
www.ceop.police.uk/safety-centre/

- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Althorpe and Keadby Primary will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
 - o act in accordance with our child protection policy and the relevant KSCMP procedures.
 - o store any devices involved securely.
 - o immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - o ensure that the DSL (or deputy) is informed.
 - o ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.

- o ensure that any copies that exist of the image, for example in emails, are deleted.
 - o report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
 - o ensure that the DSL (or deputy) is informed.
 - o ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.
 - o inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
 - o only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
 - o report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
 - o ensure that the headteacher is informed in line with our managing allegations against staff policy.
 - o inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
 - o quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at school.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at school and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

- **Online radicalisation and extremism**

As listed in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

- If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.



Acceptable Use Agreement Staff, Governor and Visitor 2021-2022

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that my use of digital technology and communications systems in school is monitored.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use deemed 'reasonable' by the Headteacher or Governing Body.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of on CPOMs and alert the Computing Lead.

I will be professional in my communications and actions when using ICT systems:

- Whilst using Google Drive I will be respectful and professional when accessing and working on shared documents and folders
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- If personal equipment is used to record these images, these must be deleted off the device/from any cloud storage as soon as possible

When publishing online, names of children will not be used.

- I will only communicate with students / pupils and parents / carers using official school systems (Gmail @akprimary.co.uk/Seesaw/School Twitter). Any such communication will be professional in tone and manner.

-
- When using the school Twitter account, log in details remain private and tweets remain professional. Any reports to be made to the Computing lead.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with or may compromise my professional responsibilities.
- I will ensure that the reputation of the school is not brought into question, following any messages, blogs or posts I may make online.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment.
- I will not use personal email addresses on the school ICT systems for school purposes.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission has been granted by the Computing coordinator/technician.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will respect copyrights and intellectual property rights.
- I will immediately report any damage or faults involving equipment or software, to the Computing lead

The school has the legal responsibility to comply with GDPR:

- I will not save *personal* or *sensitive* data onto a memory stick which is taken away from school unless it has been encrypted.

- I will make sure that personal or sensitive data I am working on at home will not be stored on a personal device but will be saved to Google Drive.
- I will take reasonable measures to keep data secure (locking your computer when out of the room/logging out of your Google account).
- I understand the responsibility for data once hardware is no longer used and I will take steps to delete or wipe devices such as USBs and laptops.
- I have read and will follow the information set out in the school's GDPR policy.
- I understand that the GDPR policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- If a breach of data has occurred, I know I have a responsibility to report this to the GDPR officer (Gillian Bush)

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

User Signature

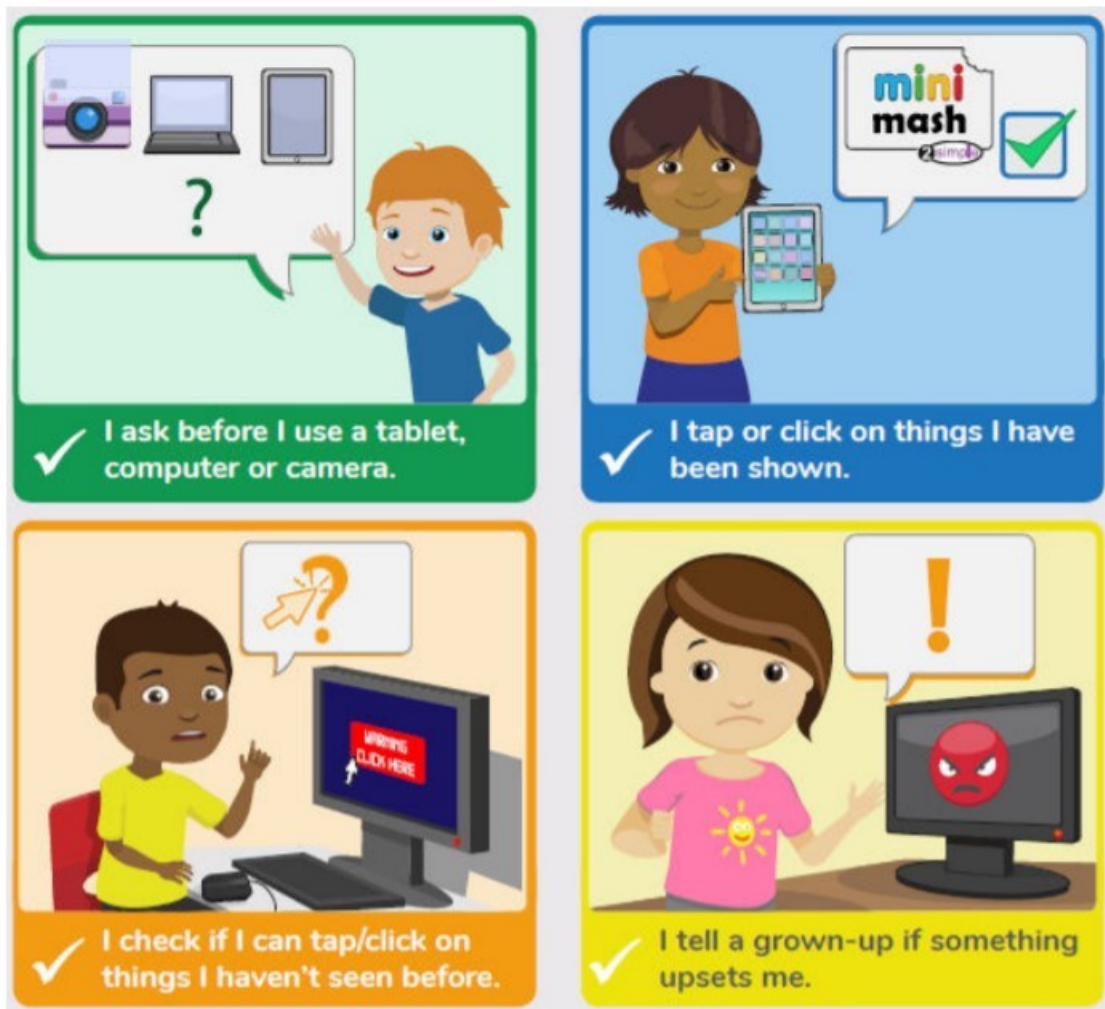
I agree to follow this code of conduct and support the safe use of ICT throughout the school.

Signature_____

Date _____

Full Name (printed) _____

EYFS Online Acceptable Use Agreement



Key Stage 1

- I am always polite and friendly when talking online.
- I only open activities that an adult has told or allowed me to use.
- I keep my usernames and passwords safe and will never use anyone else's.
- I know personal information like my address or birthday should never be shared online.
- I will treat the iPads and laptops with care.
- When I have finished on an app (e.g. spelling shed)

I will log out before the next person uses it.

- I will ask a friend for permission before I take photographs or videos of them.
- If I see something that upsets me, I must close the laptop or iPad and tell a grown up.

I know that my parent / carer will be contacted if a member of staff is worried about my online safety or behaviour.

Key Stage 2

- I will keep usernames and passwords safe by making sure they are not shared with others.
- I will not share personal information about myself or others when online.
- I will log out of websites /apps and laptops when I have finished.

- I will respect others' work and will not open, copy, remove or change any of it.
- I am responsible for my own behaviour online and know that the rules are there to keep myself safe.
- I will not take or share pictures or videos of anyone without their permission.

- I will make sure that information I post online will put no one at risk, including myself.
- I will report any aggressive or inappropriate behaviour to a member of staff.
- If I find something inappropriate online, I will close my laptop or iPad and tell a member of staff immediately.
- I will check with an adult if a pop up or attachment appears.
- I will not install or try to install apps or software on any school device, or try to change computer settings.

I know that my parent / carer will be contacted if a member of staff is

worried about my online safety or behaviour.