Eastfield Primary School
E-safety Policy

Key Details

Designated Safeguarding Lead (s): Sarah Hay

Online Safety Lead: Rachael Barnett

Date written: September 2023

Date agreed and ratified by Governing:

Date of next review: September 2024

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents
Online Safety Policy Template Content

Eastfield Primary School Online Safety Policy

1. Policy aims

- This online safety policy has been written by Eastfield Primary School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice from Online Behaviours Ltd.
- It takes into account the DfE statutory guidance [Keeping children safe in education 2023 (publishing.service.gov.uk)](publishing.service.gov.uk) [Early years foundation stage (EYFS) statutory framework - GOV.UK (www.gov.uk)](www.gov.uk)'Working Together to Safeguard Children' and DfE 'Safeguarding and remote education during coronavirus (COVID-19)'
- Eastfield Primary School follows safeguarding principles in accordance with [Keeping children safe in education 2023 (publishing.service.gov.uk)](publishing.service.gov.uk) and related guidance.
- The purpose of Eastfield Primary School's online safety policy is to
    - safeguard and promote the welfare of all members of Eastfield Primary School community online.
    - identify approaches to educate and raise awareness of online safety throughout our community.
    - enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - identify clear procedures to follow when responding to online safety concerns.

- Eastfield Primary School identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk.
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commerce:** the use of a child's data without their informed consent, and the ease with which children can be drawn into accepting legal contracts or spending money online.

2. Policy scope

- Eastfield Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

- Eastfield Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- Eastfield Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct policy
    - Positive Behaviour for Learning policy
    - Safeguarding policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data protection & GDPR policy
    - Remote learning policy
    - Preventing Extremism and Radicalisation policy.

3. Monitoring and review

- Technology evolves and changes rapidly; as such Eastfield Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher/DSL will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Sarah Hay (Headteacher) is recognised as holding overall responsibility for online safety.
- The Computing and E-safety Leader (or Online Safety Lead), Rachael Barnett, is the appointed leader and first point of contact for E-safety issues within school.
- Eastfield Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team, supported by the Online Safety Lead (OSL) will:

- Create a whole setting culture that incorporates online safety throughout all elements of 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 and E-services support 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.

4.2 The Designated Safeguarding Lead (DSL) supported by the OSL 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.
- 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, as appropriate, to the school management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding/online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read 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.
- 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.

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

- Provide technical support and perspective to the DSL and 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.

4.5 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.
- 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.

4.6 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- 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 the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as social media platforms 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.

5.   Education and engagement approaches

5.1 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 delivery is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework 2020' and DfE 'Teaching online safety in school' guidance.
    - o ensuring online safety is addressed, where appropriate, within 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 such as Digital Ambassadors.
    - 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 if appropriate.
    - o rewarding positive use of technology using appropriate in-school policies and systems.

- Eastfield Primary School 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.
    - 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.

- Eastfield Primary School 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:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.
    - 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.
    - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation as well as how to avoid infringing copyright and plagiarism.
    - enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - preparing them to identify possible online risks and make informed decisions about how to act and respond.
    - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners

- Eastfield Primary School recognises 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.
- Eastfield Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners. The Wolverhampton Learning Technology Team's E-learning framework and Project EVOLVE resources form the core of the online safety curriculum.
- Staff at Eastfield Primary School will seek input from specialist staff as appropriate, including the OSL, DSL, SENCO and RSE Leader to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will
    - provide and discuss the online safety policy, AUPs and procedures with all members of staff as part of induction.
    - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be achieved via:
        - Annual safeguarding training
        - Annual online safety briefing

- Ongoing professional development such as EPICT
- Regularly as part of staff meetings
- Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
  - build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
  - make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
  - make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
  - highlight useful educational resources and tools which staff could use with learners.
  - 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.

5.4 Awareness and engagement with parents and carers

- Eastfield Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by
  - providing information and guidance on online safety in a variety of formats. This will include:
    - Specific online safety briefings
    - Parent/carer workshops/accreditation
    - Newsletters
    - The school website and social media channels
    - Parents' evenings
  - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement
  - requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Eastfield Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will
  - regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.

- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
  - 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. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- Eastfield Primary School uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices
  - Internet, which may include search engines and educational websites
  - Email
  - Games-based technologies
  - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
  - All staff laptops and external hard drives are encrypted
  - All iPads are managed using device management software to allow remote wiping, locking and location detection. Pupils cannot install or delete apps. All iPads have passwords which are regularly changed. Pupil content is wiped from devices regularly.
- Members of staff will always evaluate websites, (particularly YouTube – https://safeyoutube.net/ or https://safeshare.tv will be used to ensure a safe experience), tools and apps fully before use in the classroom or recommending for use at home. New apps will only be allowed following a suitable risk assessment.
- The setting will use appropriate search tools as identified following an informed risk assessment. **SWGfL Swiggle** will be used as the default search engine up to and including Year 6. Other search engines may be used in years 5 & 6 with appropriate safe searching activated as default, once pupils have been shown how to search safely and how to report any concerning search results.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners age and ability.
  - **Early Years Foundation Stage and Key Stage 1**

- ▪ Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

    o **Key Stage 2**
        - ▪ Learners will use age-appropriate search engines and online tools.
        - ▪ Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing internet access

- We will maintain a written record of users who are granted access to our devices and systems, including Wi-Fi.
- 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.

7.3 Filtering and monitoring

7.3.1 Decision making

- Eastfield Primary School 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.
- 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.

7.3.2 Appropriate filtering

- Eastfield Primary School uses Lightspeed filtering.
    o Lightspeed 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 Lightspeed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    o Lightspeed integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

We work with Wolverhampton E-services 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
  - report the concern immediately to a member of staff who will report the URL of the site to technical staff/services.
  - Staff should record this as a safeguarding issue depending on the circumstances
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners **as appropriate.**
- 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.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - e.g. physical monitoring (supervision)
  - monitoring internet and web access (reviewing logfile information)
  - Eastfield Primary School uses Senso, a cloud based filtering program, which alerts the DSL to any usage of filtered language in school immediately with a screenshot of the device screen.
- 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 respond swiftly in line with the safeguarding & child protection policy.

7.4 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.
  - Full information can be found in our Data Protection and GDPR policy.

7.5 Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - 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.
  - Not using portable media eg memory sticks/external storage devices. (if memory sticks are permitted, they must be encrypted and appropriate virus checks should be run when inserted)
  - 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 eg staff will not disable proxy settings whilst in school or link to mobile phones
o The appropriate use of user logins and passwords to access our network.
   ▪ Specific user logins and passwords will be enforced for all users.
o All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 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.
- From year 3, all learners will be provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
   o use strong passwords for access into our system.
   o Alert the OSL if they suspect it has been compromised.
   o not share passwords or login information with others or leave passwords/login details where others can find them.
   o not to login as another user at any time.
   o lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE https://www.gov.uk/guidance/what-maintained-schools-must-publish-online or
- https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-online
- 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.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Use of images and videos, including online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) data security, acceptable use policies, codes of conduct/behaviour, (use on social media and use of mobile devices is covered later).

- Written permission from parents or carers (and learners where possible) will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, **the personal equipment of staff should never be used for such purposes.**
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

7.8 Managing email

- 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.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. Staff should only use recognised school email systems in relation to work.
- School 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 the Headteacher/DSL/OSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 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 school business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email.

7.8.2 Learner email

- If required, learners will use a school provided email account for educational purposes.
- Learners will discuss and agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Staff emails will be used for communication outside of the setting eg. with an author or external organisation.

7.9 Remote / online learning

- This section links to the school's Remote Learning plan and policy.
- Eastfield Primary School uses a range of online learning resources, all of which have been risk assessed before being made available to learners.
- The school website, it's Youtube channel and Rising Stars reading scheme are used as the school's online learning environment. All users discuss and agree the school's AUP before use.
- Parents/carers will be informed about the use of the learning environment and encouraged to support their child in contributing positively and reporting issues should they occur.
- Staff should also be aware of their role in maintaining a professional online environment.
- Should any member of staff wish to conduct a 'live' video lesson at any time (eg where remote learning activities are required for all or some pupils due to school closure), this should be discussed with senior leaders/DSL/OSL to ensure the correct systems are put in place (to see these processes in detail, please see the Remote Learning plan/policy)
- Systems are in place to ensure the correct pupils have access and other pupils cannot join teams/classes without being added by members of staff.

7.10 Management of applications (apps) used to record children's progress

We use SIMS, DC Pro and Class Charts to track learners progress and share appropriate information with parents and carers.

- The Headteacher will 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

o only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.

o 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.

o 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.

o all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

o 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.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Eastfield Primary School 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 Eastfield Primary School community are expected to engage in social media in a positive and responsible manner.
    - o All members of Eastfield Primary 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.
- We will control learner and staff access to social media whilst using school provided devices and systems on site.
    - o Pupils cannot access social media using school devices or whilst connected to school Wi-Fi. Selected staff may be given access on school devices eg to Twitter/Facebook to allow updating of the school's official social media channels.
    - o The use of social media during teaching/PPA hours for personal use is not permitted for staff.
    - o The use of social media during school hours for personal use is not permitted for learners.
    - o Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.
- Concerns regarding the online conduct of any member of Eastfield Primary 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 safeguarding & child protection policies.

8.2 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.

8.2.1 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 Eastfield Primary 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.

8.2.2 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.
- All members of staff are expected not to communicate with, or add, any current or past learners or their family members as 'friends' on any personal social media sites.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with 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 headteacher (or deputy DSL).

8.3 Learners use of social media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
  - o to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
  - o to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  - o not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
  - o to use safe passwords.
  - o to use social media sites which are appropriate for their age and abilities.
  - o how to block and report unwanted communications.
  - o how to report concerns on social media, both within the setting and externally.

8.4 Official use of social media

- Eastfield Primary School official social media channels are:
  - o Facebook
  - o Youtube
- The official use of social media sites by Eastfield Primary School 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.
  - o Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

- o Staff use school provided email addresses to register for and manage official social media channels.
- o Official social media sites are suitably protected
- o Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- 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.
  - o Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - o Any official social media activity involving learners will be moderated.
- 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.

8.4.1 Staff expectations
- Staff are expected not to like or comment on posts from the official school social media using their personal accounts as this might make them visible to parents and pupils.
- 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 Sign our social media acceptable use policy.
  - 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 (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

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

- Eastfield Primary 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.

9.1 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 Eastfield Primary 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 Eastfield Primary 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 Eastfield Primary 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.

9.2 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 (e.g. locked in a locker/drawer) 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.
- Staff will only use school provided equipment (not personal devices):

- o to take photos or videos of learners in line with our image use policy.
- o to work directly with learners during lessons/educational activities
- o to communicate with parents and carers.
- Where remote learning activities are required because of Covid-19, staff will use school provided equipment.
- 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.

9.3 Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - o Mobile phones may not be brought into school.
    - o Eastfield Primary School expects learners' personal devices and mobile phones to remain off-site, and if found they will be held by the class teacher until the end of the day.
- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, online safety, behaviour or anti-bullying policy.
    - o Searches of mobile phone or personal devices will be carried out in accordance with our policy and in line with the DfE 'Searching, Screening and Confiscation' guidance.
    - o Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - o Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the day (week, term etc)
    - o If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' use of personal devices and mobile phones

- All visitors/contractors will leave their phone in their pocket and turned to silent. If required to take a call, visitors must move to an agreed area free from children.
- Under no circumstances will it be used (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students.

- If required (e.g. to take photos of equipment or buildings), visitors will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- Appropriate signage and information is provided to inform parents/carers and visitors of expectations of use.

- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or Headteacher of any breaches of our 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.
  - 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 Local Authority Designated Officer.
- 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 and/or Headteacher will speak with the police and/or the Local Authority Designated Officer first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 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.
- Eastfield Primary 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.

10.2 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/code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer 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.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

  - o Our headteacher, 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 2023 (publishing.service.gov.uk) ' Full details of our response to child-on-child sexual violence and sexual harassment can be found in our safeguarding & child protection policy.
- Eastfield Primary School recognises 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 and policy.
  - 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 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.
- Eastfield 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.
- Eastfield Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Eastfield Primary School 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.

11.2 Youth produced sexual imagery ("sexting")

- Eastfield Primary 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: [Sharing nudes and semi-nudes Advice for education settings working with children and young people Responding to incidents and safeguarding children and young people.](#)
    - 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.
    - 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.
- Eastfield Primary School 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 eg the school website, internal platforms, staff room.
- 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:
    - 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.
    - 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:
    - act in accordance with our child protection policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the [UKCIS](#) guidance.
    - 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.
    - carry out a risk assessment in line with the [UKCIS](#) 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 partner services and/or the police, as deemed appropriate in line with the [UKCIS](#) 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.

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

- Eastfield Primary School 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.
- Eastfield Primary School 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 on our website.
- 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 partner services 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 from the Local Authority Designated Officer 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.

11.4 Indecent Images of Children (IIOC)

- Eastfield Primary School 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.

11.5 Online bullying

- Online bullying, along with all other forms of bullying, will not be tolerated at Eastfield Primary School.
- Full details of how we will respond to online bullying are set out in our anti-bullying policy.

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Eastfield Primary 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 Local Authority Designated Officer and/or the police.

11.7 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.

Useful Links

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

Appendices

- Student / Pupil Acceptable Use Agreement template (older children)

- Student / Pupil Acceptable Use Agreement template (younger children)

- Parents / Carers Acceptable Use Agreement template

- Staff and Volunteers Acceptable Use Agreement Policy template

- Eastfield Primary School Privacy Notice

Pupil Acceptable Use Agreement – for older pupils (KS2)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

• I understand that the school will monitor my use of the systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)

• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

• I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so

I will act as I expect others to act toward me:

• I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

• I will not use social media sites when in school.

When using the internet for research or recreation, I recognise that:

• I should ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not try to download copies (including music and videos)

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

•   I use the school systems and devices (both in and out of school)

•   I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc

•   I use my own equipment out of the school in a way that is related to me being a member of this school

 eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Group / Class

Signed

Date

Parent / Carer Countersignature:

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):………………………………………….…

Signed (parent): ………………………………………..

Parent / Carer Acceptable Use Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
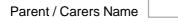
• that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name ☐   Student / Pupil Name ☐

As the parent / carer of the above pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I understand that I have a responsibility to ensure that my own online activities do not bring the school or any individuals within the school into disrepute. I also understand that I should not make reference to the school, its staff or any of its pupils in relation to school activities (including digital images / video). I understand that the school is within its rights to take appropriate action if deemed necessary.

Signed [   ]   Date [   ]

<u>Photographs and digital film recording – Parent Consent Form</u>

Within school we use photographs and digital images for a number of reasons. The use of digital / video images now play a very important part in learning activities. Pupils and members of staff may use digital cameras / ipads to record evidence of activities in lessons and out of school. Teachers may then use these images in presentations in subsequent lessons.

The main purpose of images within Eastfield Primary is to celebrate the success of pupils and so Images may be used to celebrate success through their publication in letters, on the school website and occasionally in the public media.

Photographs are used on classroom and corridor display boards, life channel screens (on the playground and the front of school) and also on the school website e.g. photographs of pupils learning, sports teams and school productions / celebrations / festivals.

Photographs are also used in Children's Learning Journeys in Reception and also in children's exercise books to gather evidence of your child's learning.

From time to time our school may be visited by the media who will take photographs or film footage of a visiting important person or another high profile event. Children will often appear in these images, which may appear in local or national newspapers or on televised news programmes.

We will always take great care to only show photographs if we feel the medium is appropriate. To comply with the Data Protection Act 1988, we need your permission before we can photograph or make any recordings of your child and so therefore I am writing to ask for your consent to use photographs and film in the following ways at Eastfield Primary School:

- School website. This will include the prospectus, school letters and curriculum documents. The website photos shows school visits, trips and enrichment activities, and celebrates children's success/celebration e.g. celebration assemblies and extra curricular activities etc. No child will

be named on the school's website alongside their image.

- Images made available to purchase via the Internet by an external photographer (where applicable) e.g. class photographs

- Displays (classroom and corridor) within the school (to include Life Channel screens – not connected to the internet)

- Learning Journeys and exercise books

- Press articles

If you need clarification or are concerned about the use of your child's photograph please contact the school.

Please complete the table below by circling 'yes or no' next to each statement, sign and date the form and then return the form to school by <mark>XXXXX</mark>

I give permission for my child's photograph to be used within school for learning and celebration purposes - on classroom and corridor displays and in children's exercise books	YES / NO
I give permission for my child's photograph to be used on the school's website	YES / NO
I give permission for my child to appear in the media e.g. Express and Star, Wolverhampton Chronicle	YES / NO
I give permission for my child to have a class photograph taken and understand that this class photograph can be purchased by parents	YES / NO

<u>Consent is assumed indefinite. However, you do have the right to withdraw consent at any time by writing to the Head Teacher.</u>

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, **nor should parents / carers publish images / video or comment on any activities involving other pupils**.

Name of child…………………………….. Class   .....

Signed   parent/carer   ....………….Date   ....

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

•   that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

•   that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

•   that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

•   I understand that the school will monitor my use of the ICT systems, email and other digital communications.

•   I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.

•   I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

•   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, to the appropriate person.

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

•   I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

•   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. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

•   I will only use chat and social networking sites in school in accordance with the school's policies.

•   I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

•   I will not engage in any on-line activity that may compromise my professional responsibilities.

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 / 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 also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

•   I will not use personal email addresses on the school ICT systems.

•   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 ensure that my data is regularly backed up, in accordance with relevant school policies.

•   I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) 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 this is allowed in school policies.

•   I will not disable or cause any damage to school equipment, or the equipment belonging to others.

•   I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

•   I understand that data protection policy requires that any staff or 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.

•   I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

•   I will ensure that I have permission to use the original work of others in my own work

•   Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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 ICT equipment in school, but also applies to my use of school ICT 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, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing principle of GDPR, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the school website https://www.eastfieldprimaryschool.org.uk/gdpr.

Parents / carers of young people who are new to the school will be provided with a link to the notice.

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;

- Judging the level of the risks (both the likelihood and consequences); and

- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	
PROTECT	1 or 2	Will apply in schools
RESTRICTED	3	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (school laptops).

Portable data storage (e.g. memory sticks, flash drives) must not be used for the storage of personal or school data.

Private equipment (ie owned by the users) must not be used for the storage of personal or school data.

When personal data is stored on any portable computer system:

• the data must be encrypted and password protected,

• the device must be password protected

• the device must offer approved virus and malware checking software.

• the data must be securely deleted from the device once it has been transferred or its use is complete.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

• Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

• Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

• When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform:

• If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location:

• Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and

•   Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

<u>Disposal of data</u>

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Use of technologies and Protective Marking

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendix – Eastfield Primary School Privacy Notice

GDPR PRIVACY NOTICE For Pupils and their Parents of Eastfield Primary School

Who processes your information?

Eastfield Primary School is the data controller of the personal information you provide to us. This means the school is responsible for deciding how information you provide us with is used. We refer to your information as "personal data" and when we use your information in different ways, this is called "processing". The General Data Protection Regulation (GDPR) outlines how personal data should be protected and used appropriately by organisations. In some cases, your personal data will be shared with other people, organisations or companies. This sharing will only occur after we have sought your permission (consent), unless the law requires us to do so. If we share your personal data outside of school, we ensure that the same data protection standards are upheld by other people involved in processing your personal data.

The categories of pupil information that we process include:

· personal identifiers and contacts (such as name, unique pupil number, contact details and address)

· characteristics (such as ethnicity, language, and free school meal eligibility)

· safeguarding information (such as court orders and professional involvement)

· images (such as photographs and CCTV images)

· special educational needs (including the needs and ranking)

· medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)

· attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)

· assessment and attainment (such as Key Stage 1 and 2 and phonics results)

· behavioural information (such as exclusions and any relevant alternative provision put in place)

Why do we collect and use your information?

Eastfield Primary School holds the right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, local authorities and / or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

· Article 6 and Article 9 of the GDPR

· Education Act 1996

· Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of pupils and their families is collected and used for the following reasons:

· To support pupil learning

· To monitor and report on pupil progress

· To provide appropriate pastoral care

· To assess the quality of our service

· To comply with the law regarding data sharing

· To keep children safe (food allergies, or emergency contact details)

· To meet the statutory duties placed upon us for DfE data collections

Which data is collected?

· Personal information – e.g. names, pupil numbers and addresses

· Characteristics – e.g. ethnicity, language, nationality, country of birth and free school meal eligibility

· Attendance information – e.g. number of absences and absence reasons

· Assessment information – e.g. national curriculum assessment results

· Relevant medical information

· Information relating to SEND

· Behavioural information – e.g. behaviour incidents and temporary exclusions

· Photographs – these will be used to aid our records management, safeguarding and attendance procedures

· Assessment and examination information

· Welfare and other pastoral support information

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. The school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used. The categories of parent information that the school collects, holds and shares includes the following:

· Contact information, including addresses, phone numbers and email

addresses of parents and/or any other emergency contacts

· Financial information where appropriate, e.g. to check eligibility for FSM

· Information pertaining to home life where appropriate, e.g. where a pupil is identified as having a mental health issue or there are safeguarding concerns

How long is your data stored for?

Personal data relating to pupils at Eastfield Primary School and their families is stored in line with the school's GDPR Data Protection Policy. In accordance with GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which is was originally collected. We will also retain personal data in the form of images, registers and examples of work for the purposes of archiving and as a historical record of school life. This information may later be published in school literature, displays or external media. In this case, the personal data we retain will be proportionate and limited to what is necessary.

Will my information be shared?

The school is required to share pupils' data with the DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with the DfE under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013. The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Eastfield Primary School is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

· Conducting research or analysis

· Producing statistics

· Providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supportinginformation Eastfield Primary School does not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. The school routinely shares pupils' information with:

· Pupils' destinations upon leaving the school

· Wolverhampton Council and its agencies (Social Services, Admissions & Appeals)

· The NHS and other health professionals (School Nurses)

· The Department of Education

· Other Government agencies (Ofsted)

· External Support Agencies (Welfare support, Inclusion and Behaviour Services)

· The providers of our management information system (Capita SIMS)

· The software we use to communicate with you (Teachers2Parents)

· The system we use for managing visitors to school (Osbourne Technologies)

· Our virtual learning environment (Cloudw / E-services)

· The systems we use for recording progress in learning (Mathletics, Doodle Maths, Lexia)

· The online software we use to help us manage the classroom (Edukey)

· The online software we use to help us manage visit and health & safety (Evolve)

· Local Authority Auditors (Wolverhampton LA)

· Visit/trip providers (Swimming/Activity Centres)

· Sports Coaches (Wolverhampton Wanderers Foundation)

· Alternative Education Providers

· Education Phycologists (Illuminate Psychology)

· School Photographer (Aperture)

· Contract Catering Services (Wolverhampton LA)

· Auditors (Wolverhampton LA)

· Contract Data Management Services (S4S)

· Contract IT Support Services (E-Services)

What are your rights?

Parents and pupils have the following rights in relation to the processing of their personal data. You have the right to:

· Request access to the personal data that Eastfield Primary School holds

· Object to processing of personal data that is likely to cause, or is causing, damage or distress

· Prevent processing for the purpose of direct marketing

· Request that your personal data is amended if it is inaccurate or incomplete

· Request that your personal data is erased where there is no compelling reason for its continued processing

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

Where can you find out more information?

For more information about the Department of Education's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data For information about which organisations the Department of Education has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-recieved

To contact the DfE: https://www.gov.uk/contact-dfe

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact our Data Protection at DPO@eastfieldpri.co.uk or by writing to Eastfield Primary School, Colliery Rd, Wolverhampton WV1 2QY.

Please address letters: For the attention of the Data Protection Officer.

You also have the right to:

· object to processing of personal data that is likely to cause, or is causing, damage or distress

· prevent processing for the purpose of direct marketing

· object to decisions being taken by automated means

· in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and

· a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/ Contact

If you would like to discuss anything in this privacy notice, please contact: DPO@eastfieldpri.co.uk or by writing to Eastfield Primary School, Colliery Rd, Wolverhampton WV1 2QY.