Huncote Primary School

Online Safety policy

(Non-statutory)

Introduction

Key people / dates

Designated Safeguarding Lead (DSL) team	Mrs Rachel Cumberlidge
Online-safety lead (If different)	
Online-safety / safeguarding link governor	Jacqui Stretton
PSHE/RSHE lead	Mrs Rachel Cumberlidge
Network manager / other technical support	Mr Michael Jones / Mr Joe Baum
Date this policy was reviewed and by whom	Reviewed Sept by Mrs Jodie Chadwick
Date of next review and by whom	September 2023 by Mrs Jodie Chadwick

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the school statutory Safeguarding Policy. Any issues and concerns with online safety **must** follow the school's safeguarding and child protection procedures. This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area.

This policy is always accessible to and understood by all stakeholders. It will also be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers.
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

This policy aims to:

- Set out expectations for all Huncote Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and

    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

What are the main online safety risks today?

New technologies have become integral to the lives of children and young people in today's society, both in school and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of the wider world which promote effective learning. Children and young people always have an entitlement to safe internet access. As such, regular monitoring is carried out.

The requirement to ensure that children and young people can use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The development and implementation of such a strategy involves all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put children at risk in and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. This policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher - (Mrs Rachel Cumberlidge)

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding leads and ensure that the DSL and DDSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with all safeguarding leads on all online-safety issues which might arise and receive regular updates on school issues.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead /Deputy Designated safeguarding/ lead Online Safety Lead– (Mrs Rachel Cumberlidge/ Mrs Sally Houghton)

Key responsibilities:

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"
- Work with the HT and technical staff to review protections for **pupils in the** and **remote-learning** procedures, rules and safeguards.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN in a college and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown
- Oversee and discuss 'appropriate filtering and monitoring' with and ensure staff are also aware
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers

Governing Body, led by Online Safety / Safeguarding Link Governor – (Louise Owen)

Key responsibilities

- Approve this policy and strategy and subsequently review its effectiveness.

- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguard.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

All staff

Key responsibilities:

- Have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices.
- Have read, understood and signed the Staff Acceptable Use Policy and Remote Learning Policy
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Report any suspected misuse or problem to the DSL
- Ensure that all pupils understand and follow the Online Safety Policy and Acceptable Use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- In 2021 pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies**.

- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Computing Lead – (Mrs Jodie Chadwick)

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Data Protection Officer (DPO) –(John Walker)

Key responsibilities:

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
  "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

- Keep a log the Embrace MAT portal and report any data breaches and corrective actions to MAT's solicitor.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Make sure that all staff members, governors and volunteers are aware of the risks of data breaches and taking the correct precautions.
- Ensure that all staff members, governors and volunteers have read and understood the Breach Management Flowchart.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read and promote the pupils' acceptable use policy and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

Education and curriculum

The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE). At Huncote this is taught through the scheme of Jigsaw.
- Computing. At Huncote this is taught through the scheme of Teach Computing.
-

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

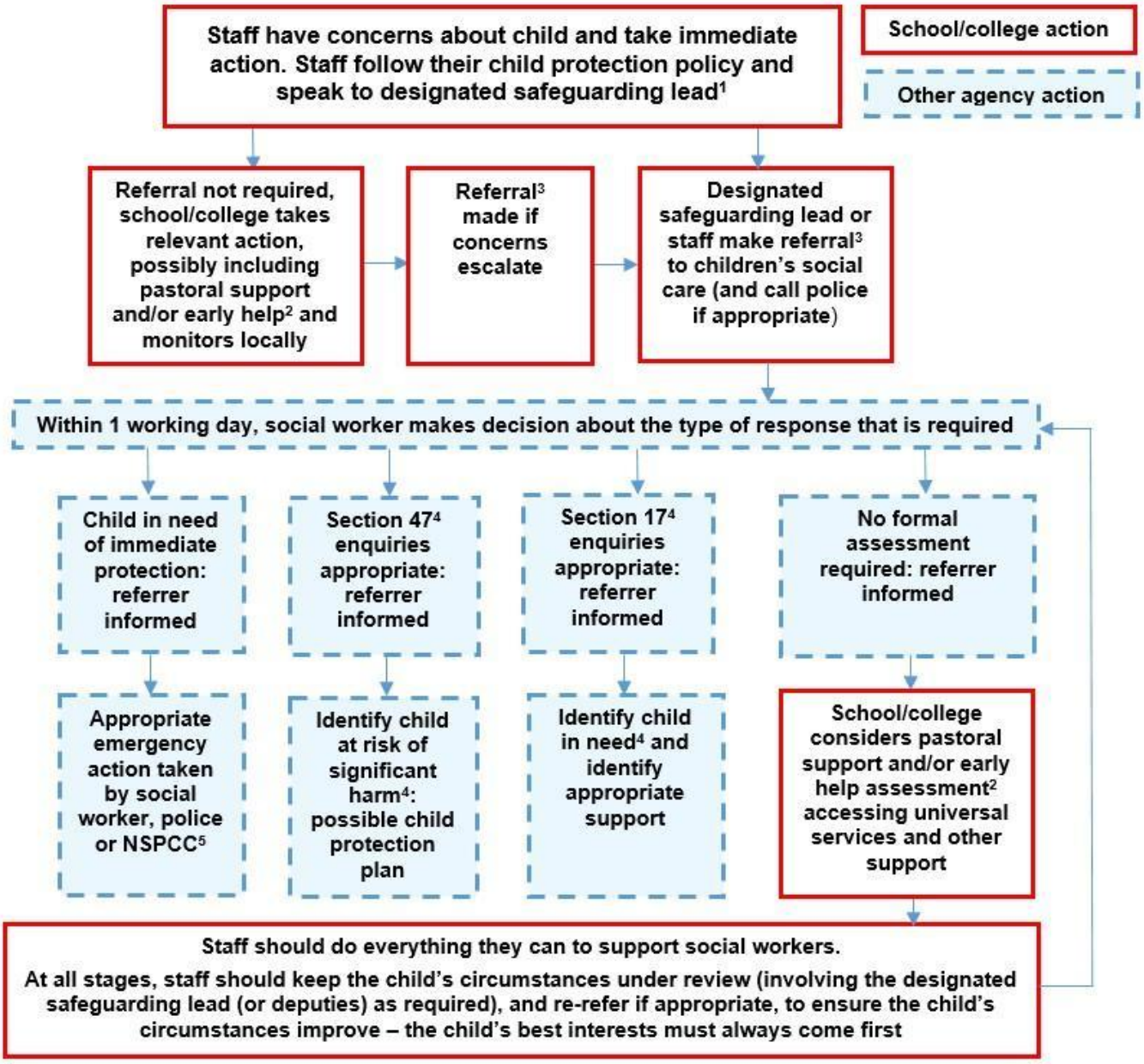
Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting.

At Huncote Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 22 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

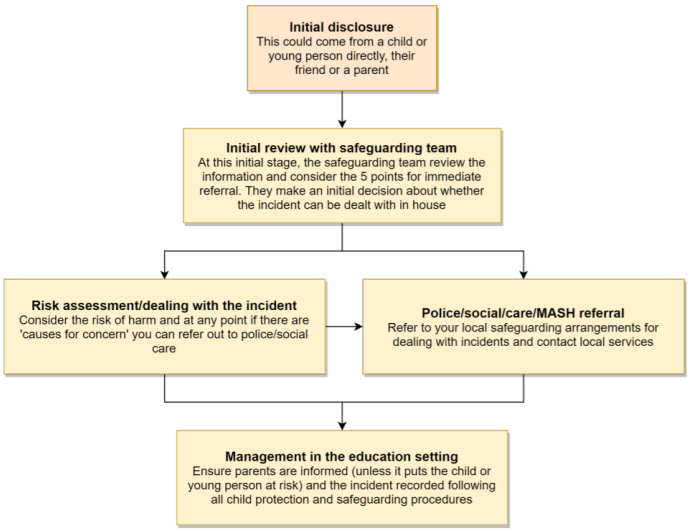


Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils should feel comfortable to come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. Please see Anti-Bullying Policy for more information.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

Social Media breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff) as well as Social Media Code of Conduct for Parents/Carers and the Wider Community.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community. Huncote Primary school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Huncote Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Rachel Cumberlidge is responsible for managing our Twitter and Class Dojo accounts and checking our Wikipedia and Google reviews. She follows the appropriate guidelines to ensure the school's reputation reminds untarnished.

Embrace IT services

At Huncote, our monitoring and filter services, emails, internet and school website are dealt with by Embrace IT Services (EITS) who provide us with a School Service Level Agreement please see policy in appendix B.

Email

Staff at Huncote Primary should use the Staff E-Mail system for all school emails. This system is linked to and fully auditable, trackable and managed. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff.
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO should be informed immediately
- Staff or pupil personal data should never be sent/shared/stored on email unless password protected
- rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value.

The DfE has determined information which must be available on a school website. **Note that an RSHE policy is now included.**

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For use in paper-based school marketing
- For online prospectus or websites
- For a specific professional image released to families for sale
- For social media
- Class dojo

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Huncote, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Appendix A

1. Safeguarding and Child Protection Policy- file:///C:/Users/jchadwick/Downloads/5.-Safeguarding-and-Child-Protection-Policy-2021-2022-Sept-2021-Version.pdf
2. Behaviour Policy - file:///C:/Users/jchadwick/Downloads/8.-Behaviour-Policy.pdf
3. Staff Code of Conduct / Handbook
4. GPDR policy - file:///C:/Users/jchadwick/Downloads/16.-GDPR-Data-Protection-Policy-2021-2022.pdf

5. Education for a Connected World cross-curricular digital resilience framework – https://www.gov.uk/government/publications/education-for-a-connected-world

6. Working together to safeguard children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Appendix B

Embrace IT Services (EITS)

School Service Level Agreement

Time Allocation

Time has been allocated to schools proportionally based on need, size of school and amount being paid into the service. The time allocations for each school for the academic year 2020/2021 can be found below:

	Weekly Allocation	Scheduled Day
Arnesby Primary School	2 Hours	Tuesday PM
Brockington College	7.4 Hours	Thursday
Croft Primary School	3.5 Hours	Monday PM
Huncote	3.5 Hours	Wednesday AM
Manorfield Primary School	6 Hours	Monday AM, Wednesday PM
Sherrier Primary School	6 Hours	Friday
St Peters Primary School	4 Hours	Tuesday AM
Additional allocation for central team work and schools needing increased support	4.6 Hours	

Please note the above is a provisional allocation and it is important to note:

- Requirements across the trust will be regularly monitored to ensure the level of support is appropriate to the need of the school and that the time allocated is suitable for a high-level of support. We will provide all schools with a 6 and 12 monthly online review (survey) to ensure that the level of support is suitable. Where the level of support is not suitable, potential changes to time allocation and costs will be discussed with the headteacher.

- Days of the week are provisional and flexible. The aim is to keep some flexibility, should a school need urgent support and assistance

- There are additional days outside of normal term-time where project work will take place to ensure schools' needs are being met. The allocation of this time will be broadly inline with the above ratio, but will be dependent on where need is greatest

Backups

All schools are different and therefore have differing needs relating to backups.

Where online backups are suitable and financially viable, critical school files will be backed up using Microsoft Azure Cloud Backups in a secure and encrypted manner.

Where online backups are not financially viable due to the size of storage required, a suitable on-premises alternative will be discussed with the school.

In both instances, schools will be provided with a document which details comprehensively which files and folders are being backed up, how they are backed up (whether locally, or in the cloud) and how long they are stored for. This is to be signed by the headteacher, so it is clear which areas EITS are responsible for protecting.

The retention period used by all schools within the trust will be based around the following standard:

Backup Type	Retention Period
Daily Backup	30 Days
Weekly Backup	4 Weeks
Monthly Backup	3 Months
Yearly Backup	1 Year

The price of backing up data varies depending on the amount of storage used. Approximate current costs are £50pa for 10gb, £130pa for 100gb and £600pa for 1000gb. An accurate pricing calculator can be found here: https://azure.microsoft.com/en-gb/pricing/calculator/. The estimated amount needed will be discussed with individual schools during the setup phase, so that costs are not unexpected.

EITS will check to ensure backups are functioning correctly on a monthly basis, and perform a test file recovery on a 3 monthly basis to ensure data consistency.

Management Information System - Bromcom

Whilst all schools have a direct support contract with Bromcom, Embrace IT Services will provide a second-line support service for any issues, training queries or day-to-day administration of the Bromcom MIS. The team will also assist with any escalations, should schools feel that Bromcom are not meeting their contractual obligations or would just like further support.

If you have any complaints, queries or training requests regarding Bromcom please log them through the helpdesk and we will deal with your query as promptly as possible.

EITS will also offer one-off sessions when it is beneficial to all (or most) schools to do so (end of year, for example)

Data Security

Data protection and ensuring good data practices remain the responsibility of the school through the Data Protection Officer (DPO).

None the less the EITS team will endeavour to support online data protection by:

- working with the DPO to ensure good data practice
- making recommendations to schools, either individually or as a group regarding recommendations and best practice
- helping to deliver staff INSET where requested and appropriate, to ensure good data security measures are being adopted

EITS will also work with all schools to ensure their most sensitive online data is protected by Multi-Factor Authentication.

Email Systems

EITS are responsible as the first point of contact for any queries relating to your email system. We will support in all aspects of email management including, but not limited to, ensuring all email is routed appropriately, all necessary users have email accounts, any filters in place are appropriate and the development of email addresses and sign-offs that are linked to the trust/school.

Network Structure

EITS are responsible for ensuring any network infrastructure is secure, fit for purpose and reliable. Where upgrades are necessary or required, we will work to specify a programme of upgrades, conduct a tender process where necessary and ensure the school implements a solution which is good value for money.

EITS will be working towards a standard network infrastructure wherever possible, in order to simplify maintenance and provide a higher level of service for all. Details of this infrastructure will be published as a supplementary document.

Website

EITS offer a web design and consultancy service to help schools ensure they have a modern and intuitive website.

See the below links as examples:

https://www.brockington.leics.sch.uk

http://www.stpeterswhetstone.co.uk/

Costs for this vary depending on the complexity of the site and can be discussed/priced as required.

Website hosting and minor updates/support is included within the Service Level Agreement, if website design services have been purchased from EITS.

Alternatively, schools may wish to stay with their current providers, and continue any external support contract they have in place with third parties.

Procurement Windows & Recommended Hardware

In order to leverage value for money and economies of scale across the trust, there will be predefined purchasing windows for new and replacement hardware throughout the year.

Prior to each purchasing window EITS will review the market and talk to suppliers to provide a list of best value recommended hardware covering Desktops, Laptops, Monitors & AV. Where schools have specific requirements, EITS will work closely to provide solutions within this purchasing window. Procurement must go through EITS and not be undertaken by any school independently.

Support Desk Service

EITS offer an online support desk service in order to effectively and efficiently prioritise the requirements of all schools. This can be accessed via the following address:

http://www.brockington.leics.sch.uk/primaryhelpdesk/

It is important that all support is logged through this system to maximise the service that we can offer.

Acceptable Use Policy

EITS, in conjunction with Trust Leaders, will lead in the creation, promotion and adherence to a Trust-Wide Acceptable Use Policy.

The Acceptable Use Policy, based around Local Authority templates, industry wide standards and trust specific procedures aims to safeguard staff and students, ensure compliance with GDPR/data protection guidelines and ensure the best use of the computer systems provided. This policy will be reviewed centrally at least every two years.

It will be the schools individual responsibility to track acceptance of the AUP and ensure it is signed by all members of staff with computer accounts.

Telephony

Telephony remains outside the scope of the Service Level Agreement. EITS will however work with individual schools at the point of contract expiry to review options and support the renewals process to implement the best value solution for individual schools.

Internet Connectivity

Internet connectivity is reviewed on a regular basis and will focus around cost, speed of connection and quality of filtering among other things.

Benefits of group purchasing, including decreased cost due to economies of scale, the ability to provide more secure infrastructure over private networks mean that where possible a single supplier will be used across the trust.

The ability to allow exceptions to internet filtering will be delegated to individual schools, but EITS will also support by adding exceptions where necessary.

Complaints

If you have any complaints regarding the service you are receiving from EITS then please contact Michael Jones via ITServiceLead@embracemat.org in the first instance. Alternatively you can contact the trust leader on tl@embracemat.org if more appropriate.

Annex 1

Individual School Backup Agreement Policy

School Name:_____

The following is a comprehensive list of network drives which are to be backed up in an encrypted manner using the online Microsoft Azure backup platform. It details the area on the server, that will be backed up and any specific exceptions which exist.

Please discuss the below carefully with a member of the EITS team, ensure you are happy with what is being backed up and is capable of being recovered in a disaster recovery scenario.

Data Area Storage	Specific Inclusions	Specific Exclusions	Approx Storage

Price of backing up data varies depending on the amount of storage used. Approximate current costs are £50pa for 10gb, £130pa for 100gb and £600pa for 1000gb. Accurate pricing calculator can be found here: https://azure.microsoft.com/en-gb/pricing/calculator/

Onsite Backups

We recommend backing up all essential data to the cloud whenever possible and within the constraints of budget restrictions. We appreciate for larger storage capacity this is not always possible and EITS will always endeavour to work with schools and backup data on-site. Details of what is backed up on-site, and how, can be found below.

Data Area Storage	Specific Inclusions	Specific Exclusions	Approx Storage

Brief details of onsite backups

Please check over the above and ensure you are happy with backup details listed. If you are unsure on any of the above, please speak to a member of the EITS team. Once happy please sign the below:

Signed: _____

Date: _____