

Hardwick Primary School

Online Safety Policy

Contents	Page no
1. Policy Aims	3
2. Legislation and guidance	3
3. Policy Scope	3-4
3.1 Links with other policies and practices	4
4. Monitoring and Review	4
5. Roles and Responsibilities	4
5.1 The governing body	4-5
5.2 The Headteacher and leadership and management team	5
5.3 The Designated Safeguarding Lead	5-6
5.4 Members of staff and volunteers	6
5.5 Staff who manage the technical environment	6-7
5.6 Learners	7
5.7 Parents and carers	7
6. Education and Engagement Approaches	7
6.1 Educating pupils about online safety	7-9
6.2 Vulnerable Learners	9
6.3 Training and engagement with staff	9-10
6.4 Awareness and engagement with parents and carers	10
7. Reducing Online Risks	10
8. Safer Use of Technology	11
8.1 Classroom Use	11
8.2 Managing Internet Access	11
8.3 Filtering and Monitoring	11
8.3.a Decision Making	12
8.3.b Filtering	12
8.3.c Monitoring	12
8.4 Managing Personal Data Online	13
8.5 Security and Management of Information Systems	13
8.5.a Password policy	13
8.6 Managing the Safety of our Website	13-14
8.7 Publishing Images and Videos Online	14
8.8 Managing Email	14
8.8.a Staff email	14
8.8.b Learner email	14
8.9 Educational use of Video conferencing and/or Webcams	14
8.10 Management of Learning Platforms	15
8.11 Management of Applications (apps) used to Record Children’s Progress	15
9. Social Media	16
9.1 Expectations	16
9.2 Staff Personal Use of Social Media	16-17
9.3 Learners Personal Use of Social Media	17-18
9.4 Official Use of Social Media	18-19

Hardwick Primary School Online Safety Policy

10. Use of Personal Devices and Mobile Phones	19
10.1 Expectations	19-20
10.2 Staff Use of Personal Devices and Mobile Phones	20
10.3 Learners Use of Personal Devices and Mobile Phones	21
10.4 Visitors' Use of Personal Devices and Mobile Phones	21
10.5 Officially provided mobile phones and devices	21-22
11. Responding to Online Safety Incidents and Concerns	22
11.1 Concerns about Learners Welfare	22
11.2 Learners and Staff Misuse	22-23
12. Procedures for Responding to Specific Online Incidents or Concerns	23
12.1 Online Sexual Violence and Sexual Harassment between Children	23-24
12.2 Youth Produced Sexual Imagery ("Sexting")	24-25
12.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)	25-26
12.4 Indecent Images of Children (IIOC)	26-27
12.5 Cyberbullying	27
12.6 Online Hate	29
12.7 Online Radicalisation and Extremism	29
13. Useful Links for Educational Settings	29-30
Appendix 1: EYFS and KS1 acceptable use agreement	31
Appendix 2: KS2 acceptable use agreement	32
Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)	33
Appendix 4: Online safety training needs – self audit for staff	34
Appendix 5: online safety incident report log	35

This policy was reviewed/amended: September 2020

Next review: September 2021

Hardwick Primary School

Online Safety Policy

1. Policy Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear procedures to identify, intervene and escalate an incident, where appropriate

Hardwick Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Hardwick Primary School

Online Safety Policy

3. Policy Scope

- Hardwick Primary School believes 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.
- Hardwick 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.
- Hardwick Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- 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, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

3.1 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Child protection and Safeguarding policy
- Behaviour and discipline policy
- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Staff Code of conduct
- Staff disciplinary procedures
- Confidentiality policy
- Data protection policy and privacy notices
- Complaints procedure
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)

4. Monitoring and Review

- Technology in this area evolves and changes rapidly. Hardwick Primary School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the 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 Designated Safeguarding Lead will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

5. Roles and Responsibilities

Hardwick Primary School

Online Safety Policy

5.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Andy Abbott.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- The Designated Safeguarding Lead (DSL) Nick Wells has lead responsibility for online safety.
- Hardwick Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

5.2 The Headteacher and leadership and management team

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

They will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

5.3 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.

Hardwick Primary School

Online Safety Policy

- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date 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.
- 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, policies and procedures.
- Report online safety concerns, as appropriate, to the setting 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 and online safety.

5.4 It is the responsibility of all members of staff and volunteers to:

- Contribute to the development of online safety policies.
- Read and Implementing this policy consistently and adhere to the acceptable use policies.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and 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 children in their care.
- Take personal responsibility for professional development in this area.

Hardwick Primary School

Online Safety Policy

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material, whilst allowing learning opportunities to be maximised.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

5.7 It is the responsibility of parents and carers to:

- Read the acceptable use 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.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

6. Education and Engagement Approaches

Hardwick Primary School

Online Safety Policy

6.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

From September 2020 all schools will have to teach:

- ❖ [Relationships education and health education](#) in primary schools

This new requirement includes aspects about online safety.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

Hardwick Primary School

Online Safety Policy

- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

6.2 Vulnerable Learners

- Hardwick Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Hardwick Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum Hardwick Primary School will seek input from specialist staff as appropriate, including the SENDCO and Child in Care Designated Teacher.

6.3 Training and engagement with staff

We will:

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings). This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety 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.

Hardwick Primary School Online Safety Policy

- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

The Online Safety Lead will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

6.4 Awareness and engagement with parents and carers

Hardwick 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 offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and school events.
- Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they 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.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

7. Reducing Online Risks

Hardwick 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.

Hardwick Primary School

Online Safety Policy

- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- 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 to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

8. Safer Use of Technology

8.1 Classroom Use

Hardwick Primary School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - Email
 - Games-based technologies through apps
 - Digital cameras, web cams and video cameras via iPads
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
 - Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
 - The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
 - 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 learners will be appropriate to their 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.

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.

8.2 Managing Internet Access

Hardwick Primary School

Online Safety Policy

- All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8.3 Filtering and Monitoring

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

8.3.a Decision Making

- Hardwick Primary School leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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.

8.3.b Filtering

- Education broadband connectivity is provided through Schools Broadband.
- We use 'Smooth Wall' which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with SCC and Schools Broadband to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
 - Turn off monitor/screen and report the concern immediately to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.

Hardwick Primary School

Online Safety Policy

- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Suffolk Police or CEOP.

8.3.c Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
 - Monitoring of internet and web access through reviewing of log information.
- If a concern is identified via monitoring approaches we will:
 - Raise the concern with the DSL or deputy who will respond in line with the Behaviour and Child Protection Safeguarding policy.
- 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.

8.4 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 school's information security policy.

8.5 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 without specific permission; portable media will be checked by an anti-virus /malware scan before use.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on our network,
 - The appropriate use of user logins and passwords to access our network.
 - Specific user logins and passwords will be enforced for all but the youngest users.
 - All users are expected to log off or lock their screens/devices if systems are unattended.

8.5.a Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year R, all learners have their own unique username. In Year 4, learners create their own private passwords to access our systems; learners are then responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.

Hardwick Primary School

Online Safety Policy

- Change their passwords every six weeks
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

8.6 Managing the Safety of our Website

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

8.7 Publishing Images and Videos Online

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

8.8 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 policies and the code of conduct/behaviour policy.
 - The forwarding of any chain messages/emails is not permitted.
 - Spam or junk mail will be blocked and reported to the email provider.
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
 - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL 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.

8.8.a Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.

Hardwick Primary School

Online Safety Policy

- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

8.8.b Learner email

- Learners are not currently provided with school email accounts for educational purposes. If that changes in the future, learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

8.9 Educational use of Video conferencing and/or Webcams

- Hardwick Primary School does not currently use video conferencing or webcams.

8.10 Management of Learning Platforms

Hardwick Primary School uses Microsoft 365 as its official learning platform.

- Staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff will have access to the LP.
- When staff leave the setting, their account will be disabled or transferred to their new establishment.
- Staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- If the content is illegal, we will respond in line with existing child protection procedures.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.
- Supply teachers and any other temporary staff members, who need computer access during their visit to Hardwick Primary School, will be supplied with a generic account and password, which will give them limited access to the school's network.

8.11 Management of Applications (apps) used to Record Children's Progress

Hardwick Primary School

Online Safety Policy

- We use Primary Target Tracker to track learners progress and share appropriate information with parents and carers.
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

9. Social Media

9.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Hardwick 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 Hardwick Primary School community are expected to engage in social media in a positive, safe and responsible manner.
- All members of Hardwick Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
 - The use of social media during setting hours for personal use is not permitted.
 - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Hardwick Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Hardwick Primary School

Online Safety Policy

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing 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 code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
 - 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 sites. 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):
 - Setting the privacy levels of their personal sites.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Hardwick Primary School on their personal social networking accounts; this is to prevent information on these sites from 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 and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Headteacher.

Hardwick Primary School

Online Safety Policy

- 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.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

9.3 Learners Personal 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 state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
 - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

9.4 Official Use of Social Media

Hardwick Primary School does have twitter and Facebook accounts, however they are not currently used. The school uses ClassDojo instead. If the school decides to use twitter and/or Facebook as a form of communication, the following will also apply.

The school's official social media channels are:

○ <https://twitter.com/>

○ <https://www.facebook.com/pages/Hardwick-primary-school>

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.

Hardwick Primary School

Online Safety Policy

- 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 social media sites or accounts for educational or engagement purposes only.
 - Staff use setting provided email addresses to register for and manage any official social media channels.
 - Official social media sites are suitably protected and, where possible, run and are linked to our website.
 - 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: anti-bullying, image/camera use, data protection, confidentiality and child protection.
 - All communication on official social media platforms 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.
 - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving learners will be moderated possible.
- 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.

Class Dojo

ClassDojo is an online application that is provided free to parents/carers, so they be involved in the learning of their child at school. Parents/carers can either access the site through the App or via the website. They will be issued with a code linked to their child's class, so only parents/carers from that class can see the posts from the school. A member of school staff must be officially verified by the school and ClassDojo before gaining access. The DSL/Headteacher monitors all content put on class pages. Information about ClassDojo safety, privacy and GDPR compliance can be found on their website www.classdojo.com

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - Sign our social media acceptable use policy.
 - Always be professional and aware they are an ambassador for the setting.
 - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.

Hardwick Primary School

Online Safety Policy

- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

10. Use of Personal Devices and Mobile Phones

Hardwick Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

10.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection and safeguarding.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - All members of Hardwick Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - All members of Hardwick 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 other than in the staff room or in personal offices. They must never be used in teaching areas or on the playground/field.
- 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 as part of our behaviour policy.
- All members of Hardwick 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.

Hardwick Primary School

Online Safety Policy

10.2 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.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
 - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff school are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and/or Headteacher.
- Staff will not use personal devices:
 - To take photos or videos of learners and will only use work-provided equipment for this purpose.
 - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/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, the police will be contacted.

10.3 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.
- Hardwick Primary School expects learners' personal devices and mobile phones to be to be used in accordance with the acceptable use policy.
- Learner's in Upper Key Stage 2 personal mobile phones and personal devices will be handed into the school office to be kept in a secure place during the school day and collected at the end of the day. Learners in other year groups are not permitted to bring personal devices mobile phones to school.
- If a learner needs to contact his/her parents or carers they will be allowed to use the school phone.
- Parents are advised to contact their child via the school office

Hardwick Primary School

Online Safety Policy

- Mobile phones or personal devices will not be used by learners during lessons.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
 - Searches of mobile phone or personal devices will only be carried out in accordance with our policy. See www.gov.uk/government/publications/searching-screening-and-confiscation
 - 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. www.gov.uk/government/publications/searching-screening-and-confiscation
 - 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.

10.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use mobile phones and personal devices in accordance with the school Acceptable Use Policy.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

10.5 Officially provided mobile phones and devices

- The setting does not have or provide mobile phones to members of staff.
- If contact with learners or parents/ carers is required, staff will use the school phone in the office or email from the school admin account.

11. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must 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.

Hardwick Primary School

Online Safety Policy

- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or Suffolk Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headteacher will speak with Suffolk Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

11.1 Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Suffolk Safeguarding Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11.2 Learners and Staff Misuse

- Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use – The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy. Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Procedures for Responding to Specific Online Incidents or Concerns

12.1 Online Sexual Violence and Sexual Harassment between Children

Hardwick Primary School

Online Safety Policy

- Our setting has accessed and understood “Sexual violence and sexual harassment between children in schools and colleges” (2018) guidance and part 5 of ‘Keeping Children Safe in Education’ 2020.
- Hardwick Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Hardwick 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.
- Hardwick Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Hardwick 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 between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- 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 online sexual violence and sexual harassment, we will:
 - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
 - If content is contained on learner’s electronic devices, they will be managed in accordance with the DfE ‘searching screening and confiscation’ advice.
 - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
 - Implement appropriate sanctions in accordance with our behaviour policy.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - If appropriate, make a referral to partner agencies, such as Children’s Social Work Service and/or the Police.
 - If the concern involves children and young people at a different educational setting, 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 Suffolk Police first to ensure that investigations are not compromised.
 - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Hardwick Primary School Online Safety Policy

12.2 Youth Produced Sexual Imagery (“Sexting”)

- Hardwick Primary School recognises youth produced sexual imagery (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 UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#).
- Hardwick Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ 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 youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image 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 Suffolk Safeguarding Child Board’s procedures.
 - Ensure the DSL (or deputy) responds in line with the [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Store the device securely.
- If an 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 which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Children’s Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.
 - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance’.

Hardwick Primary School

Online Safety Policy

- 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.
 - 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.

12.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Hardwick Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Hardwick Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal 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 sexual abuse and exploitation (including criminal 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 and intranet.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
 - Act in accordance with our child protection and safeguarding policy and the relevant Suffolk Safeguarding Partnership's procedures.
 - If appropriate, store any devices involved securely.
 - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Suffolk police via 101, or 999 if a child is at immediate risk.
 - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
 - 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Hardwick Primary School

Online Safety Policy

- Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report:
www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Suffolk 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 [Child Sexual Exploitation Team](#) (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Suffolk Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

12.4 Indecent Images of Children (IIOC)

- Hardwick Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- 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 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 Suffolk Police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
 - Act in accordance with our child protection and safeguarding policy and the relevant Suffolk Safeguarding Partnership's procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Suffolk police via 101 (using 999 if a child is at immediate risk).
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - Ensure that the DSL (or deputy) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - 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:
 - Ensure that the DSL (or deputy) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.

Hardwick Primary School

Online Safety Policy

- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
 - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
 - Quarantine any devices until police advice has been sought.
 - Follow the appropriate school policies regarding conduct.

12.5 Cyberbullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Hardwick Primary School.
- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationship and Health Education and personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Hardwick Primary School

Online Safety Policy

12.6 Online Hate

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

12.7 Online Radicalisation and Extremism

- 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 child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with the Prevent Duty and our child protection and safeguarding 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 Prevent Duty and our child protection and safeguarding policy.

13. Useful Links for Educational Settings

Suffolk Support and Guidance for Educational Settings

Suffolk Safeguarding Partnership:

www.suffolkscb.org.uk

Suffolk Police:

<https://www.suffolk.police.uk/advice/cyber-crime/personal-online-safety>

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

www.suffolk.gov.uk/community-and-safety/staying-safe-online/e-safer-suffolk/

National Links and Resources for Educational Settings and Parents

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

Hardwick Primary School Online Safety Policy

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- Childline: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- National Online safety: <https://nationalonlinesafety.com>
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

Hardwick Primary School

Online Safety Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

Pupils in EYFS and KS1 are not permitted to bring a mobile phone to school. Other personal electronic devices e.g. tablets, gaming devices, etc. are not permitted in school:

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using mobile phones and electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Hardwick Primary School

Online Safety Policy

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Pupils in UKS2 may bring their mobile phone to school. Pupils in other year groups are not permitted to bring a mobile phone to school. Other personal electronic devices e.g. tablets, gaming devices, etc. are not permitted in school:

- I will turn my mobile phone off when I enter school premises and hand my mobile phone in to the class teacher for safe storage.
- I will use my mobile phone responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.
- I will not use my mobile phone to take photos or video of people and post them online, including social media sites, without the express permission of the person in the photo or video.
- I will use my mobile phone responsibly and not use it cause upset to other people or use it in a way that could be viewed or classified as online bullying.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using mobile phones and electronic devices and will make sure my child understands these.

Signed (parent/carer):

Date:

Hardwick Primary School

Online Safety Policy

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Hardwick Primary School

Online Safety Policy

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Any other comments:	

