# Stanton Community Primary School

*Nurture, Enjoy, Aspire, Achieve*

## Acceptable Use and Mobile Phone Policy

| | | | |
|---|---|---|---|
| **Date of Governor Approval:** | April 2024 | **Date for Next Review:** | April 2025 |
| **Signed by:** | | | (Chair of Governors) |

Stanton Community Primary School recognises that IT and the Internet are tools for learning and communication that can be used to enhance the curriculum, challenge students, and support creativity and independence.

At Stanton Community Primary School we provide pupils with a broad and balanced curriculum that promotes the spiritual, moral, social and cultural (SMSC) development of our pupils.

Pupils will be encouraged to regard people of all faiths, genders, races and cultures with respect and tolerance.

Our guiding principle is in the education of our community *about* ***User Responsibility*** as this enables:

- the educational use of the new e-technologies available;
- the respectful use of e-technologies with regard to Stanton Community Primary School's ethos and the fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths; beliefs together with gender;
- the safe use of e-technologies so that all users are kept safe from harm

Using IT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and IT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies and devices. We know that some adults and young people will use these technologies to harm others. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children. Educating all members of the school community on the responsibilities and risks of online safety falls under this duty.

It is important that there is a balance between controlling access to the internet and e- technologies and allowing freedom to explore and use these tools to their full potential.

This policy aims to be an aid in regulating IT activity in School, and provide a good understanding of appropriate IT use that members of the School community can use as a reference for their conduct online outside of School hours.

Cyber bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in the local School **Behaviour for Learning Policy** and **Anti-Bullying policy**.

Finally, the Computer Misuse Act 1990 identifies three specific offences:

- Unauthorised access to computer material (that is, a program or data).
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
- Unauthorised modification of computer material

If the Computer Misuse Act 1990 is breached then a student or member of staff is likely to have the matter referred to other authorities including the police.

Online safety is a whole-school issue and responsibility. Please refer to other relevant policies, i.e. policies covering Data Security, Code of Conduct, etc

## Roles and Responsibilities

### Governing Bodies

The Governors are responsible for the approval of the Acceptable Use Policy and for reviewing the effectiveness of the policy by reviewing online safety provision. Online safety falls within the remit of the Governor responsible for Safeguarding.

The role of the Governors will include:

- To ensure an Acceptable Use Policy incorporating Online safety is in place, reviewed annually
- and is available to all stakeholders.
- The policy may be reviewed more frequently if significant changes occur with technologies in use
- in the Academies. The online safety policy is referenced within other School policies e.g. the Safeguarding and Child Protection Policy.
- To ensure that procedures for the safe use of IT and the Internet are in place and adhered to.
- To receive and challenge the annual online safety audit toward improvements, referring to the Critical Security Control checklist (NCC Online Safety Policy February 16 – see Appendix 10.)
- To hold the Headteacher and staff accountable for Acceptable Use / Online safety practice

### Online safety Co-ordinator

The Online safety Co-ordinator will be a role delegated to a member of the Leadership Team in each school reporting to the Headteacher who has a duty of care for ensuring the safety (including online safety) of members of the school community. Any complaint about staff misuse must be referred to the Headteacher.

The Online safety Co-ordinator will:

- Ensure that they have received appropriate CEOP training.
- Ensure access to induction and training in Online safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a member of SLT.
- Ensure that pupil or staff personal data as recorded within the School management system sent over the Internet is secured.
- Work in partnership with the DFE and the Internet Service Provider and IT Provider to ensure systems to protect students are reviewed and improved.
- Ensure the IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Ensure that the relevant Governors sub-committee will receive monitoring reports from the Online safety Co-ordinator on a termly basis

**IT Technicians**

The IT Technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body's Online safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, the internet, the Virtual Learning Environment, remote access, and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or Online safety Coordinator for investigation, action, sanction or support.
- That monitoring software / systems are implemented and updated as agreed in school policies.

**Communicating School Policy**

This policy is available *on the website* for parents, staff, and pupils to access as and when they wish.

Rules relating to the code of conduct when online, and online safety guidelines, are to be displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, for example during PSHE lessons and as part of the Computing curriculum, where personal safety, responsibility, and/or development are being discussed.

Staff who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.

## Online safety Curriculum

### Teaching and Learning

The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and pupils.

Pupils should be taught what internet use is acceptable and what is not and given clear objectives for Internet use as part of the curriculum. Assemblies and also class time may be used to support this.

Pupils should be educated in the effective use of the internet by their class teachers as appropriate and in discrete Computing lessons e.g. which sites to access; how to use the internet to research; not to copy and paste large chunks of the internet, how to use the CEOP Report abuse button etc.

Pupils will be shown how to publish and present information appropriately to a wider audience, as part of their curriculum, and as appropriate to their courses.

Online safety rules will be posted in all rooms where School IT resources are used. This also includes Library.

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. The pupils should be taught that visiting any websites and communicating online leaves a 'digital footprint'. All users are to be aware that Internet traffic can be monitored and traced to the individual user. Discretion and appropriate conduct are essential.

Pupils should be taught to:

- Be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Acknowledge the source of information used and to respect copyright.
- use age-appropriate tools to search for information online
- how and why to report inappropriate conduct online / unpleasant Internet content e.g. using the CEOP Report Abuse icon

### Managing filtering

The School will set the guidance on the use of filtering. The School will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The School will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the *School online safety coordinator.* Any material found by members of the School community that

is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an internet enabled School device. The School cannot accept liability for the material accessed, or any consequences of internet access.

The School will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

The School will consider requests for access to key sites on a case by case basis.

The School will work in partnership with Suffolk Children's Services to ensure systems to protect pupils are reviewed and improved.

For more information on data protection in School, please refer to our **Data Protection Policy.**

**Parents' support**
Parents' and carers' attention will be drawn to the Online safety Policy on enrolment of their child, via Class Dojo, the School brochure and on the School web site.

Parents and carers will from time to time be provided with additional information about online E-safety. Acceptance of a place at a School confirms the agreement of parents and students to support and abide by all School policies and procedures in place and as varied from time to time.

**Handling Online safety complaints**
Any complaint about staff misuse must be referred to the Headteacher. If the complaint is about misuse by the Headteacher, it must be referred to the Chair of Governors. Complaints of Internet misuse by students will be dealt with by the appointed member of the School Leadership Team.

Concerns of a Safeguarding nature must be referred to the Designated Safeguarding Lead and their team and dealt with in accordance with school procedures.

**Cyber bullying**
The School, as with any other form of bullying, takes Cyber bullying seriously. Information about specific strategies to prevent and tackle bullying is set out in the relevant policy on Behaviour for learning policy and Anti-Bullying.

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

If an allegation of bullying involving the use of IT or any emerging technology does take place, the School will:

- Follow the policy and procedures for dealing with bullying
- Take it seriously

- Act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs or contact the service provider in order to identify the person causing concern.
- Record and report the incident
- Provide support and reassurance to the victim
- Make it clear to the person causing concern that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group.

It is important that children who have harmed another, either physically or emotionally, redress their actions and the School will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the person causing concern will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in School.

**Use of Email**

It is important that users of our email systems should be confident about the following:

- The identity of the user of the email account with whom they are communicating.
- The security of the communications and any data sent.
- That the School has access to an audit trail of the conversation in the event of any issues
- arising.

**Staff Use of Email/Class Dojo messaging**

Staff School email accounts should be used for any and all School business and most especially when communicating with students, parents and external organisations and individuals on School business. Be aware that emails have legal force i.e. what you say in an email has as much legal standing as something you write on paper.

Personal email accounts should not be used in a professional capacity.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

The forwarding of chain messages is not permitted in School.

**Internet Resources**

Internet resources that users sign up for School purposes must be done using a School email account. Students must not be granted access to any resources using any form of personal email accounts.

**The School Website**
The contact details on the website should be the School address, e-mail and telephone number. Pupils' personal information will not be published.

Staff personal information such as a School email address will not be published unless there is a statutory requirement (e.g. Headteacher, DSL, SEND/Co, etc.)

**Published Content**
The School website is viewed as a useful tool for communicating our School ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with School news and events, celebrating whole-School and personal achievements, and promoting School projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and privacy policies. No personal information on staff or pupils will be published.

For information on School policy on children's photographs published on the School website please refer to section 9 of this policy.

**Social networking**
The School will block access to social networking sites, and will educate pupils in their safe use e.g. use of passwords.

All students will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

Pupils, parents and staff will be advised on the safe use of social network spaces. Pupils will be advised to use nicknames and avatars when using social networking sites.

**Social Media, Social Networking and Personal Publishing on School IT resources**
Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. *There are various restrictions on the use of these sites in School that apply to both students and staff.*

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through curriculum areas such as IT and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The School follows general rules on the use of social media and social networking sites in School:

Pupils are educated on the dangers of social networking sites (including gaming sites) and how to use them in safe and productive ways. They are all made fully aware of the School's code of conduct regarding the use of IT and technologies and behaviour online.

Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

Official School blogs created by staff / students for the School IT resources are not to be publicly visible unless approved. They will be moderated by a designated member of staff.

Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately.

Safe and professional behaviour of staff online will be discussed at staff induction.

## Data

### Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-School and individual progress. The School collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the School will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the School needs. Through effective data management we can monitor a range of School provisions and evaluate the wellbeing and academic progression of our School body to ensure that we are doing all we can to support both staff and students.

The School will follow these principles of good practice when processing data:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive Ensure that data processed is accurate
- Not keep data longer than is necessary
- Process the data in accordance with the data subject's rights

- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the School is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the School's safeguards relating to data protection read the Data Protection Policy.

**Cloud data storage and data sharing services e.g. Google, Microsoft 365**
Data stored on any cloud data storage must not be shared unless you are confident about how the system works, and who will be able to access the data.

**Images**
Colour photographs and pupils' work bring our School to life, showcase our students' talents, and add interest to publications both online and in print. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have safeguards in place.

It is important that published images do not identify students or put them at risk of being identified.

Only images created by or for the School will be used in public and children may not be approached or photographed while in School or doing School activities without the School's permission. The School follows general rules on the use of photographs of individual children:

Under the Data Protection Act 2018 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the School parents/carers will be asked to sign a photography consent form. The School does this so as to prevent repeatedly asking parents for consent over the School year, which is time-consuming for both parents and the School. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect the use to which you are consenting.

This consent form will outline the School's policy on the use of photographs of children, including:

- How and when the photographs will be used
- For how long parents are consenting the use of the images
- School policy on the storage and deletion of photographs.

On admission, parents or carers will complete a consent form to give permission from parents or carers before names, photographs or images of pupils are published.

**A template of the consent form can be found at the end of this policy.**

Photographs that include pupils will be selected carefully and the School will look to seek to use group photographs rather than full-face photos of individual children. Pupils' full names will be avoided on publicly accessible School IT resources as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

Parents will be clearly informed of the School policy on image taking and publishing, both on School and independent electronic repositories.

Staff and external parties will be made aware of the restrictions on photographing certain students through the website and relevant policies.

**Complaints of Misuse of Photographs or Video**
Parents should follow the standard School complaints procedure if they have a concern or complaint regarding the misuse of School photographs.

**Use of photography and filming at School events.**
Parents and Carers use of photography and filming at School events. See Appendix 11.

**Mobile Phones and Personal devices**
While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly.

Some issues surrounding the possession of these devices are that they:

- can make pupils and staff more vulnerable to cyber bullying
- can be used to access inappropriate internet material
- can be a distraction in the classroom
- are valuable items that could be stolen, damaged, or lost
- can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The School takes certain measures to ensure that mobile phones are used responsibly in School.

Children are not allowed to bring mobile phones into school. Should a child knowingly do this, it will be managed through the School's Behaviour Management policy.

**Staff**
In nurseries, staff are not permitted to bring their mobile phones into areas used by children. Personal belongings, including mobile phones, should always be stored in the nursery office.

Staff should not use their personal mobile phones to contact pupils or parents either in or out of School time for any School-related purpose. The only exception would be in an emergency and it would need to be logged with the Office staff.

Staff are not permitted to take photos or videos of pupils on their personal phones. If photos or videos are being taken as part of the School curriculum or for a professional capacity, the School equipment should be used for this.

The School expects staff to lead by example. Personal mobile phones and smart watches should be switched off or on 'silent' during School hours.

**Managing Emerging Technologies**

Technology is progressing rapidly and new technologies are emerging all the time. The School will risk assess any new technologies before they are allowed in the School, and will consider any educational benefits that they might have. The School keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

**Appendix 1 The Acceptable Use Agreement - Staff and Governors**

**Preamble**
IT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT.

All new staff are expected to sign this policy on appointment and adhere at all times to its contents, including any variations as may be made from time to time. Current staff will have the opportunity to acknowledge this updated version. This work forms part of our terms and conditions.

Any concerns or clarification should be discussed with the Headteacher or the online safety coordinator.

**Scope**
This AUP applies to the responsible use of the School's IT resources and any related technologies.

1. I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities.

2. I will ensure that all electronic communications with students and staff are compatible with my professional role.

3. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.

4. I will only use the approved, secure e-mail system(s) for any School business.

5. I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted if on a pen drive/device.

6. I will not purchase or install any hardware of software without first consulting IT Support

7. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

8. Images of students and/ or staff will only be taken, stored on the School IT system and used for professional purposes in line with School policy and with the consent of the parent, carer or staff member.

9. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager, or Headteacher.

10. I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community

11. I will respect copyright and intellectual property rights.

12. I will ensure that my use of School IT resources, both in School and outside School, will not bring my professional role into disrepute. Please refer to the Code of Conduct.

13. I will support and promote the School's online safety and Data Protection and security policies and help students to be safe and responsible in their use of IT and related technologies.

14. I understand this forms part of the terms and conditions set out in my contract of employment.

15. I will not allow any other user to access my School IT account. The exception would be if IT Support or similar support service needs to resolve problems.

16. I understand that all School-owned equipment and devices must only be used by School employees.

17. I will use my School data storage area (Local and/or cloud) only for School work.

18. If I connect a personal mobile device (e.g. laptop or USB device) to the School network or to an School device, I agree to the School systems accessing that device and that they may take necessary action, including deleting.

19. I will ensure my device is locked and inaccessible should the device be left for any period of time, regardless of how short this might be.

20. I will ensure any mobile devices are kept in a secure location when they are not being used.

21. Where a Virtual Private Network connection (VPN) is provided to remotely connect an School device to the School's local network, I will take extra care in ensuring my device is safe and secure at all times and is not used by any other individual who is not an employee of the school.

22. I will report any data breaches or assumed data breaches to the Trust Data Protection Officer.

I agree to follow this code of conduct and to support the safe and secure use of IT throughout the School.

Signature …… Date …… Full Name ……

Job title . . . . . .

**Appendix 2 The Acceptable Use Agreement – Pupils**
Each School's AUP is based on the points below and described using age appropriate language.

**Preamble**
IT - in all its forms - is part of our daily life in School.
This agreement makes students aware of their responsibilities when using IT in all its forms.
All students have a School IT account which is for their *sole* use only and for which they are responsible.
All pupils must abide by these guidelines, including any variations as may be made from time to time.
All new students will sign this document as part of the enrolment form and process.
All current students will acknowledge it as part of using their IT accounts annually. Any concerns or queries should be discussed with the Headteacher or the online safety coordinator.

**Scope**
This agreement applies to all students at the School and their use of personal and School owned devices.

This is designed to keep students safe. The School Behaviour Policy sanctions will apply as necessary for any deliberate misuse of IT.

1.I will make sure that all my IT communications are responsible and sensible. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

2. I will only use IT systems in School, including the internet, e-mail, digital video, mobile technologies, etc. for School purposes.

3. I will only log on to the School network or other resources with my own user name and password. I will not let anyone else use my account.

4. I will not reveal my passwords to anyone.

5. I will report problems that I have to the School via my teacher or an IT Technician.

6. I will treat School IT equipment with respect, I understand my parents may be asked to pay for equipment that I damage.

7. I will not download or install software on School technologies. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I come across any such material I will report it immediately to my teacher.

8. I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a School project approved by my teacher.

9. Images of students and / or staff will only be taken, stored and used for School purposes in line with School policy and not be distributed outside the School network without the permission of the class teacher.

10. I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, students or others distress, nor bring the School into disrepute.

11. I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community.

12. I will respect the privacy and ownership of others' work on-line at all times.

13. I will not attempt to bypass any security on School systems, or make use of material that is not intended for student use.

14. I understand that all my use of the computers, the internet and other related technologies can be monitored and made available to my teachers or parents.

15. I will use my School data storage area (Local and/or cloud) only for School work.

18. If I connect a mobile device (e.g. laptop or USB device) to the School network or an School device, I agree to the School systems accessing that device and that they may take necessary action.

Signed:

Print Name:

Date:

# Stanton Community Primary School

*Nurture, Enjoy, Aspire, Achieve*

**Appendix 3 Acceptable Use Agreement - Parents**

Dear Parent/ Carer

Information Technology including the internet, learning platforms, e-mail and mobile technologies has become an important part of learning in our School. We expect all students to be safe and responsible when using any IT. It is essential that students are aware of safety and know how to stay safe when using any IT.

Students are expected to read and discuss this agreement with their parent or carer and then to follow the terms of the agreement, including any variations as may be made from time to time.

Any concerns or explanation can be discussed with their form or class teacher or with the online safety coordinator or the Headteacher.

Please read Appendix 2 with your child and sign this section of the form before returning it to the School.

Please be aware that acceptance of a place at any Stanton Community Primary School and enrolment of your child constitutes your acceptance and support of the IT Acceptable Use Agreement, as valid with changes from time to time, and all other School policy and procedures.

**Parent/ carer signature**
I have read this document and will support my son/daughter in following the Acceptable Use agreement to support his / her safe and responsible use of IT while at Stanton Community Primary School.

Parent/ Carer Signature …….

Student Name…….

Class …….

Date ……

# Stanton Community Primary School

*Nurture, Enjoy, Aspire, Achieve*

**Appendix 4 Photo permission form for new parents**

Stanton Community Primary School believes that celebrating the achievement of children in School is an important part of their learning experience and personal development. Taking photographs and videos of pupils for internal display and displaying pupil work enables us to celebrate individual and group successes as a School community.

We would also like to use photographs and videos of the School and its pupils to promote the good educational practice of the School.

Children's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

By signing this form, you are consenting to the use of images of your child being used in the following outlets under the terms outlined in our online safety policy:

- School publications including Class Dojo
- On the School website
- In newspapers as allowed by the School
- In videos made by the School or in class for School projects

This consent form covers consent for the duration of your child's time at the School. Once your child leaves the School, photographs and videos may be archived within the School but will not be published without renewed consent. More information regarding the storage and protection of images can be found in the School **Data Protection policy**. A full copy of the School's policy on online safety containing information on the safe use of photographs, videos, and the work of children in School can be found in the School office and on the website.

**Parental permission signature required**
Can we use your child's photograph?

- in printed publications by School within OLW CMAT
- on our website, School blogs, or the School's partnership websites either:
    - In a group or as a member of a whole School activity
    - Individually
- for publication in a newspaper and video your child within School, and display these publicly within the School, as part of the curriculum and in class
- and videos of your child to share good practice with professionals from other

**If yes, please sign here and return:**

Signed: .....
Date: .....
PRINT NAME:.....

# Stanton Community Primary School

*Nurture, Enjoy, Aspire, Achieve*

| | |
|---|---|
| **Facebook**<br>Read Facebook's rules<br>Report to Facebook<br>Facebook Safety Centre | **YouTube**<br>Read YouTube's rules<br>Report to YouTube<br>YouTube Safety Centre |
| **Instagram**<br>Read Instagram's rules<br>Report to Instagram<br>Instagram Safety Centre | **X**<br>Read X's rules<br>Reporting to Twitter |