# STANNINGTON INFANT SCHOOL

Policy for Online Safety

Agreed by Governors Oct 2017

# Stannington Infant School Policy for Online Internet Safety

## Stannington Infant School Vision:

- **To encourage a caring and positive attitude amongst the children towards all others and their environment.**
- **To provide a challenging, creative and rich curriculum which will develop curiosity, confidence and independence.**
- **To provide an inclusive, safe, secure, healthy and happy environment.**

**Philosophy**

At Stannington Infant School we aim to provide all the necessary safeguards to help ensure that everything that could reasonably be expected of the school to manage and reduce risks related to online internet safety have been addressed. The Online Safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

Digital technology is used widely throughout our curriculum and is an ever growing aspect of children's social communication and interaction out of school. New technologies capture children's imaginations and enable them to develop key skills which provide them with the opportunities to collaborate, communicate and express themselves confidently. We are committed to promoting the positive use of new technologies whilst providing pupils with the skills and knowledge that allow them to access the internet safely and responsibly. In addition to this, the school is clear in its responsibility to also draws attention to the potential risks involved with new technologies; we aim to reach out to the community in order to spread this message so parents, carers and families can evaluate their practice, review it and become role models for their children. It is crucial that parents and teachers model the best practice, so children can follow their example.

**Scope of the Policy**

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers the Headteacher, to such an extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.
This applies to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.
Keeping Children Safe in Education September. This is a statutory guidance from the Department of Education issued under section 175 of the Education Act 2002, the Education regulations 2014 and the Education Regulations 2011. The document contains information on what schools **should** do and sets out the legal duties to safeguard and promote the welfare of children. It should be read alongside statutory guidance **Working Together to Safeguard Children 2015**.
The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

**Development / Monitoring / Review of this Policy**

This policy has been developed by the school's staff team made up of:

- School Online Safety Co-ordinator
- Headteacher / Senior Leadership Team
- Computing Leader
- PSHE lead
- ICT Technical staff

Consultation with the whole school community has taken place through the following:

| | |
|---|---|
| Title | **Online internet safety Policy** |
| Version | 3.0 |
| Date | *October 2017* |
| Author | *Liz Harris* |
| This online safety policy was approved by the Governing Body on*:* | |
| Monitoring will take place at regular intervals (at least annually): | *October 2018* |
| The Governing Body will receive a report on the implementation of the policy including anonymous details of any online internet safety incidents at regular intervals: | *Safeguarding/ Online safety will be a standing item at governor curriculum meetings (on a termly basis)* |
| The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online internet safety or incidents that have taken place. The next anticipated review date will be: | *October 2018* |
| Should serious online internet safety incidents take place, the following external persons / agencies should be informed: | Sheffield Safeguarding Advisory Desk 0114 205 3535<br>Online safety Project Manager 0114 293 6945<br>Sheffield Police<br>0114 220 2020<br>Child Exploitation and Online Protection Centre (CEOP)<br>www.ceop.police.uk |

- Professional development meetings
- Class discussion
- Governors meetings
- Parent Questionnaires

**Schedule for Development / Monitoring / Review**
The school will monitor the impact of the policy using:
Logs of reported incidents
Internal monitoring data for network activity where appropriate.
Surveys / questionnaires of:

pupils (including Every Child Matters Survey)
parents / carers
staff
**Communication of the Policy**

**Publishing the policy**

This policy will be made available on the school website where it can be read electronically and downloaded as a paper copy. All staff and students who are on placement at the school will be provided with a reduced paper copy covering key points and the document will also be available from the school reception area where key policies are displayed.

**Communication**

Stannington Infant School's senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school Online internet safety policy and the use of any new technology within school.
The Online internet safety policy will be discussed with all members of staff formally.
Any amendments to the policy will be republished immediately.
Any amendments to the children's Acceptable Use Policy will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
An Online Safety training programme will be established across the school to include a regular review of the Online Safety policy.
Pertinent points from the school Online Safety policy will be reinforced across the curriculum and across all subject areas when using IT equipment within school.
The key messages contained within the Online Safety policy will be reflected and consistent within all Acceptable Use Policies in place within school.
We endeavour to embed Online Safety messages across the curriculum whenever the internet or related technologies are used embedding Online Safety into PSHE and computing sessions.
The Online Safety policy will be introduced to the pupils at the start of each school year

<u>Roles and Responsibilities</u>

We believe that Online Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to

benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Online Safety Team (Sarah Binns, Liz Harris, Paula Greensmith and Rebecca Juggins)

To ensure that the school Online Safety policy is current and pertinent.
To ensure that the school Online Safety policy is systematically reviewed at agreed time intervals.
To ensure that school Acceptable Use Policies are appropriate for the intended audience.
To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

**Responsibilities of the Senior Leadership Team:**

The headteacher (Sarah Binns) has overall responsibility for Online Safety of all members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Lead (Liz Harris).
The headteacher and Online Safety Lead are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their Online Safety roles.
The senior leadership team will receive either verbal or written monitoring reports from the Online Safety Lead.
The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious Online Safety incident.
The headteacher should receive regular update reports from the Online Safety Lead giving details of any incidents and the effectiveness of the policy.

**Responsibilities of the Online Safety Leader**

- To promote an awareness and commitment to Online Safety throughout the school.
- To be the first point of contact in school on all Online Safety matters.
- To take day-to-day responsibility for Online Safety within school and to have a leading role in establishing and reviewing the school Online Safety policies and procedures.
- To lead the school Online Safety team.
- To have regular contact with other Online Safety committees, e.g. Safeguarding Children Board
- To communicate regularly with school technical staff.
- To communicate regularly with the designated Online Safety governor (Jonathan Foster)
- To communicate regularly with the senior leadership team.
- To create and maintain Online Safety policies and procedures.
- To develop an understanding of current Online Safety issues, guidance and appropriate legislation.

- To ensure that all members of staff receive an appropriate level of training in Online Safety issues.
- To ensure that Online Safety education is embedded across the curriculum.
- To ensure that Online Safety is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safety issues to the Online Safety group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident.
- To ensure that an Online Safety incident log is kept up to date.

**Responsibilities of the Teaching and Support Staff**

- To read, understand and help promote the school's Online Safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any suspected misuse or problem to the Online Safety lead.
- To develop and maintain an awareness of current Online Safety issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, social media or mobile phones etc.
- To embed Online Safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To be aware of Online Safety issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

**Responsibilities of Technical Staff (Blue Box IT)**

- To read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any Online Safety related issues that come to your attention to the Online Safety lead.
- To develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.

- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school IT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

**Protecting the professional identity of all staff, work placement students and volunteers**

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, smartwatches, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

**When using digital communications, staff and volunteers should:**

- only make contact with children for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child eg should not give their personal contact details to children including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- not send or accept a friend request from the child on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.

- ensure that if they have a personal social networking profile, details are not shared with children in their care (making every effort to keep personal and professional online lives separate).
- not post information online that mentions the school or could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

**Responsibilities of the Designated Safeguarding Lead (DSL)**

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

**Responsibilities of Students / pupils**

- To read, understand and adhere to the school pupil Acceptable Use Policy.
- To help and support the school in the creation of Online Safety policies and practices and to adhere to any policies and practices the school creates.
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the use of mobile phones.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- To discuss Online internet safety issues with family and friends in an open and honest way.

**Responsibilities of Parents / Carers**

- To help and support the school in promoting Online Safety.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and digital images outside of school.
- To sign a home-school agreement containing the following statements:

*I/We will support the school's approach to online safety and will not deliberately send, upload or add any text, images or sounds that could upset or offend any member of the school community.*

*I/We understand that any photographs taken at school events are allowed and I/We will ensure that any images or videos taken involving children other than my/our own are for personal use only. These will not be published on the internet including social networking sites.*

*I/We understand that written consent is required for the use of any images by school of my/our children in a variety of different circumstances. This form has been completed and returned to school.*

*I have read through and signed the acceptable use agreements on behalf of my/our child(ren) on admission to the school or when amendments have been made and agree to support any actions that result in these agreements being broken by my/our child.*

*I understand I can view the school's* Online Safety *policy on the school website or ask for a copy at the school reception and support the principles set out in this document.*

**Responsibilities of the Governing Body**

- To read, understand, contribute to and help promote the school's Online Safety policies and guidance.

- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school IT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the Online Safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety activities.
- To ensure appropriate funding and resources are available for the school to implement its Online Safety strategy.

**The role of the Online Safety Governor includes:**

- regular meetings with the Online Safety Lead
- regular monitoring of Online Safety incident logs
- reporting to Governors meeting

**Responsibilities of Other Community/ External Users**

- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and IT equipment within school.

**Planning – Teaching and Learning Strategies/Organisation**

**Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

**Online Safety education at Stannington Infant School will be provided in the following ways:**

- The teaching of key Online Safety skills in every year group which will be embedded into the computing and PSHE curriculum. This will involve reminding or raising relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and

validity of information they use and the need to respect and acknowledge ownership of digital materials.

- Celebrating and promoting Online Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Children will be taught how to use a range of age-appropriate online tools in a safe and effective way: Yahooligans and Google, under adult supervision
- Reminding children about their responsibilities through an Acceptable Use Policy which every child will sign; it will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Teaching children how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, children will be guided to use age-appropriate search engines. All use will be monitored and children will be reminded of what to do if they come across unsuitable content.
- Teaching in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Teaching about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Making children aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

**All Staff (including Governors)**

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training in the form of an annual Professional Development Meetings and Basic safeguarding Training every 3 years will be made available to staff.
- An audit of the Online Safety training needs of all staff will be carried out annually by training governor and Online Safety Lead.
- All new staff receive online internet safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.
- Updates to this policy will be presented to and discussed by staff in business meetings and Governor's meetings.
- The Online Safety lead will provide advice / guidance / training as required to individuals as required.

**Parents/Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- joint Online Safety parents' meetings with Nook Lane Junior School when possible and appropraite
- newsletters
- letters
- website
- information about national / local Online Safety campaigns / literature

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Those images are only be taken on school equipment**, the personal equipment of staff must **not** be used for such purposes.

- Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Children must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Children's full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained at the start of Foundation Stage (or when a child begins to attend Stannington Infant School) before photographs of children are published on the school website.

- Children's' work can only be published with the permission of the children and parents or carers.

- When searching for images, video or sound clips, children will be taught about copyright and acknowledging ownership.

- Images uploaded to google drive from iPads will be downloaded at the earliest opportunity and erased from Google Drive as soon as possible. Images and videos should not be stored on Google Drive and must be deleted once they have been used.

- Images should not be stored on iPads and be erased at the earliest opportunity.

**Managing IT systems and access**

The school will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible.

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- Each year group have year group user names and passwords.
- Year 2 classes have individual user names and passwords.
- Members of staff will access the T Drive (school network) using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID and password. They will abide by the school AUP at all times.
- When using CPOMs staff will only log on with their individual ID and password.
- Staff will have different levels of access to CPOMS depending on level of responsibility within school.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Yorkshire and Humberside Grid for Learning.
- The school's internet provision will include filtering appropriate to the age and maturity of children.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and children will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Children will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

**Passwords**

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- Children in Foundation Stage will have a generic 'pupil' logon to all school IT equipment.
- Children in Year 1 will have a generic 'pupil' logon to all school IT equipment.
- Children in Year2 will have an individual logon and password for all school IT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school that will be changed annually.
- All children and staff have a unique, individually named user account and password to access Purple Mash.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at any time that they feel their password may have been compromised.

- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and children have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and children will have appropriate awareness training on protecting access to their personal username and passwords for IT access.
- All staff and children will sign an Acceptable Use Policy prior to being given access to IT systems which clearly sets out appropriate behaviour for protecting access to username and passwords.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords should contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

**Management of assets**

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant IT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant IT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any IT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

**Data Protection**

**Personal Data**

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

**Staff will:**

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.

- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO (Sarah Binns) and the applicable IAO (Rebecca Juggins)
- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and children will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

**Secure Transfer Process**
**Email**

- **Only school accounts** ending @stannington.sheffield.sch.uk should be used for sending and receiving school related information.
- Staff will not include personal or sensitive information within the body of an email itself, as the information sent should be by a secure method. Instead, staff will create a document (e.g. Word document) and then encrypt the document with a password and send it as an attachment with the email. A following email will be sent which informs the recipient of the password to open the attachment.

**FAX**

- Fax machines will be situated within the school office.

- No sensitive information or personal data will be sent by FAX. Instead, it will be sent by email using the method explained in bullet point 2 of Email.

**Communication Technologies**

.

A wide range of rapidly developing communications technologies has the potential to enhance learning.

| | Staff & other adults | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | √ | | | | | | | √ |
| Smartwatches may be brought into school | | √ | | | | | | √ |
| Use of mobile phones in lessons | | | | √ | | | | √ |
| Use of smartwatches in lessons | | | | √ | | | | √ |
| Use of mobile phones in social time | √ | | | | | | | √ |
| Use of smartwatches in social time | √ | | | | | | | √ |
| Taking photos/ video on school equipment | √ | | | | | √ | | |
| Taking photos/ video on personal equipment | | | | √ | | | | √ |
| Use of personal email addresses in school, or on school network | | | | √ | | | | √ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Use of school email for personal emails | | | | ✓ | | | ✓ | |
| Use of chat rooms / facilities | | | | ✓ | | | | ✓ |
| Use of instant messaging | | ✓ | | | | | | ✓ |
| Use of social networking sites in school | | | | ✓ | | | | ✓ |
| Use of blogs | | ✓ | | | | ✓ | | |

When using communication technologies the school considers the following as good practice:

- The official school email service (ending '@stannington.sheffield.sch.uk') is used to send and receive emails related to school.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and children or parents / carers (email, chat, VLE, texting etc) must be professional in tone and content.

**Unsuitable / inappropriate activities**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for certain users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | child sexual abuse images | | | | | ☐ |
| | promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation | | | | | ☐ |
| | adult material that potentially breaches the Obscene Publications Act in the UK | | | | | ☐ |
| | criminally racist material in UK | | | | | ☐ |
| | Pornography | | | | ☐ | |
| | promotion of any kind of discrimination | | | | ☐ | |
| | promotion of racial or religious hatred | | | | ☐ | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | ☐ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | ▯ | |
| Using school systems to run a private business | | | | | ▯ | |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school | | | ▯ | | | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | ▯ | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | | ▯ | |
| Creating or propagating computer viruses or other harmful files | | | | | ▯ | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | | | ▯ | |
| Use school equipment for on-line gaming (educational) | ▯ | | | | | |
| Use school equipment for on-line gaming (non educational) | | | | | □ | |
| Use school equipment for on-line gambling | | | | | □ | |
| On-line shopping / commerce - eBay etc. | | ▯ | | | | |
| Use school equipment for accessing social networking sites | ▯ | | | | | |
| Use school equipment for video broadcasting eg Youtube | | | □ | | | |

**Responding to incidents of misuse**

It is hoped that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Stannington Infant School's Online Safety flow chart should be consulted and actions followed.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows

## Pupils

## Actions / Sanctions

| Incidents: | Refer to class teacher | Refer to Online Safety lead | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction e.g. red card / exclusion |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | √ | √ | √ | | √ | | | |
| Unauthorised use of non-educational sites during lessons | √ | | | | | | | √ | |
| Unauthorised use of mobile phone / digital camera / other handheld device | √ | | | | | √ | | √ | |
| Unauthorised use of social networking / instant messaging / personal email | √ | √ | | | | √ | | | √ |
| Unauthorised downloading or uploading of files | √ | √ | | | | √ | | | √ |
| Allowing others to access school network by sharing username and passwords | √ | | | | | | | | |
| Attempting to access or accessing the school network, using another student's / pupil's account | √ | | | | | | | √ | |
| Attempting to access or accessing the school network, using the account of a member of staff | | √ | √ | | | √ | | | √ |
| Corrupting or destroying the data of other users | √ | | | | | | | √ | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | √ | √ | | | √ | | | √ |
| Continued infringements of the above, following previous warnings or sanctions | | √ | √ | | | √ | | | √ |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | √ | √ | | | √ | | | √ |
| Using proxy sites or other means to subvert the school's filtering system | | √ | √ | | | √ | | | √ |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | √ | √ | | √ | √ | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | √ | √ | | √ | √ | | | √ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | √ | √ | | | | | | | |

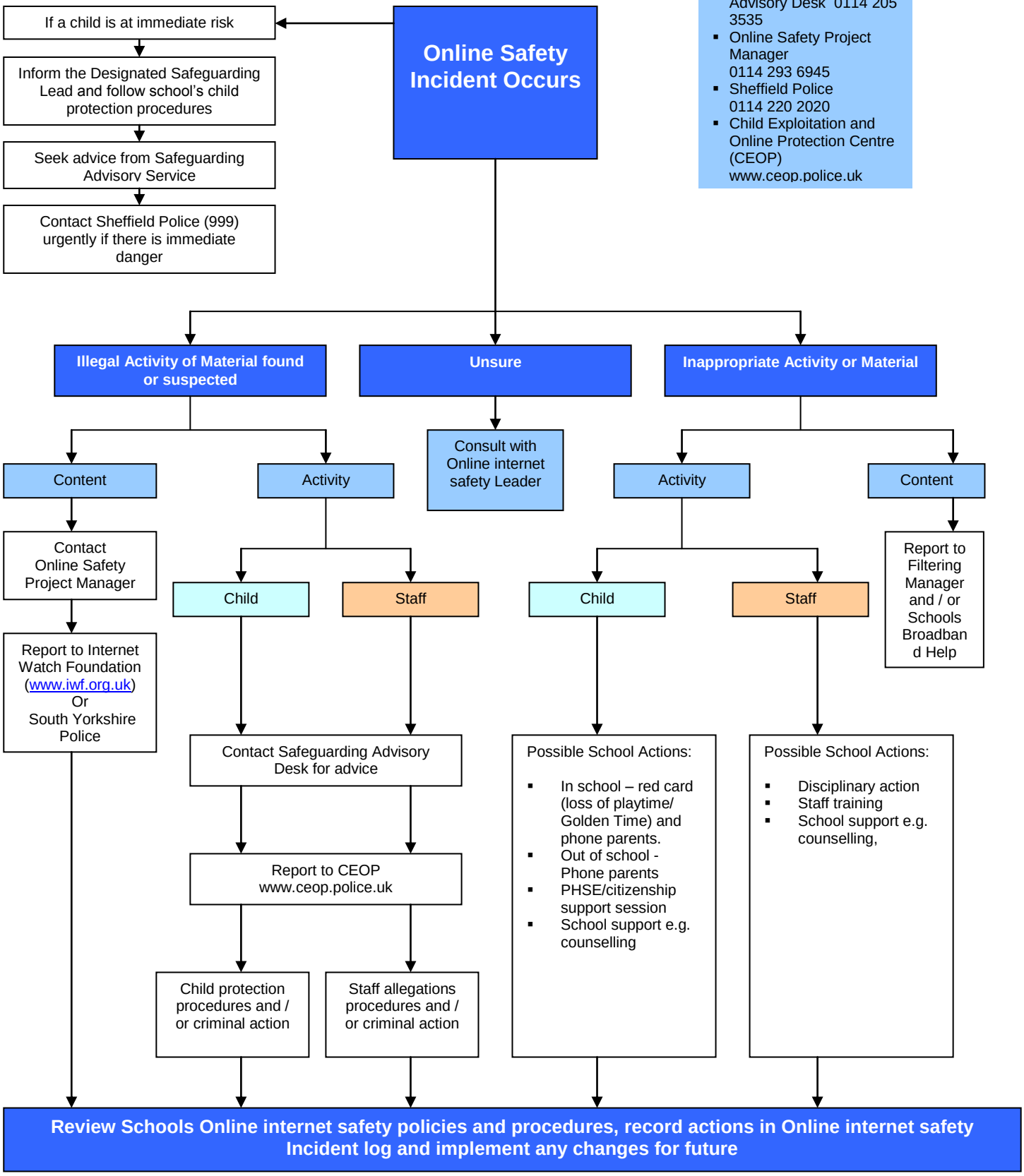
## Staff

## Actions / Sanctions

| Incidents: | Refer to Online Safety Lead | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | √ | √ | √ | | | | √ |
| Inappropriate personal use of the internet / social networking sites / instant messaging / personal email | | √ | | | | √ | | √ |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | √ | | | | | | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | √ | √ | | | | | | |
| Deliberate actions to breach data protection or network security rules | | √ | | | | √ | | √ |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | √ | | | | √ | | √ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | √ | | | | √ | | √ |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | | √ | | | | √ | | √ |
| Actions which could compromise the staff member's professional standing | | √ | | | | √ | | √ |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | √ | | | | √ | | √ |
| Using proxy sites or other means to subvert the school's filtering system | √ | | | | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | √ | √ | | | √ | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | √ | | | √ | | | √ |
| Breaching copyright or licensing regulations | √ | | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions | √ | √ | | | | √ | | |

# Response to an Incident of Concern

**Contacts**
- Sheffield Safeguarding Advisory Desk 0114 205 3535
- Online Safety Project Manager 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk




**Contact Details**

| |
|---|
| Schools Designated Safeguarding Lead Officer: Sarah Binns (Lead) Liz Harris (Deputy) |
| School Online Safety Lead: Liz Harris |
| Safeguarding Children Board safeguarding Manager: |

**Appendices**

- Staff and Volunteers Acceptable Usage Policy template
- Parents / Carers Acceptable Usage Policy Agreement template
- Use of Digital Images and sample Consent Form
- Mobile Phone Use
- Questions for Schools to consider
- Links to other organisations, documents and resources
- Legislation

**Stannington Infant School**
**Pupil Acceptable Use Policy Agreement**

**This is how we stay safe when we use computers/laptops/iPads/cameras:**

I will ask a teacher if I want to use the computers/laptops/iPads/cameras.

I will only use activities that the teacher has allowed me to use.

I will only take pictures of other children if my teacher has given me permission to do so.

I will take care of the computer and other equipment.

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

I will *tell the teacher* if I see something that upsets me on the screen.

I will use Hector to cover something up on the screen that upsets me while I fetch the teacher.

I know that if I break the rules I might not be allowed to use a computers/laptops/iPads/cameras.

Signed (child):……

Signed (parent): ……

## Stannington Infant School

## IT Acceptable Use Staff Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.
This is not an exhaustive list and all members of staff are reminded that IT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, smartwatches, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulations 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the School Image Use Policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.

- I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the, Sarah Binns (Designated Safeguarding Lead), Liz Harris (Deputy Designated Safeguarding Lead and Online Safety Coordinator) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches following the Online Safety incident flowchart.
- I will not attempt to bypass any filtering and/or security systems put in place by the school unless I have permission to view curriculum related material (e.g. YouTube access for assembly). If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the Paula Greensmith, Computing leader.
- My electronic communications with children, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- My use of IT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of IT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.
- I will promote Online Safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with Liz Harris (Online Safety Coordinator) or Sarah Binns (Head Teacher).
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

*The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood the Staff IT Acceptable Use Policy.**

Signed: …… Print Name: …… Date: ……