Online Policy

Date completed / last reviewed:	September 2023
Date for review:	September 2024
Cross Reference:	Anti Bullying Policy Behaviour and Discipline Policy Social Media Guidance Stivichall Safeguarding and Child Protection Policy Acceptable Use Policy Staff Acceptable Use Policy

Learning at Stivichall is a passport for life

Introduction

National guidance suggests that it is essential for schools to take a leading role in Online Safety.

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to government in the following areas: delivering Online Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to learners. The benefits are perceived to "outweigh the risks." However, schools must, through their Online Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

In the guidance issued to schools in September 2013, Ofsted will make a judgement on our school's ability to:

- *Protect and educate pupils and staff in their use of technology;*
- *Have the appropriate mechanisms to intervene and support any incident where appropriate.*

Ofsted categorise the breadth of issues into three broad areas of risk:

- *content: being exposed to illegal, inappropriate or harmful material;*
- *contact: being subject to harmful online interaction with other users;*
- *conduct: personal online behaviour that increases the likelihood of, or causes, harm.*

Stivichall's Online Safety policy operates in conjunction with our policies relating to student behaviour and discipline, acceptable use, anti-bullying, curriculum, data protection and safeguarding and child protection.

We are committed to making sure that the whole school community is fully involved in the issue of Online Safety. We are actively committed to making sure governors, all adults working in school, our parents and our pupils are provided with up-to-date information, guidance and strategies relating to Online Safety on our school website, twitter feed and weekly newsletter. We are also committed to ensuring that children are taught to recognise when they are at risk, and how to get help if they need it.

As with all other risks, it is impossible for our school to eliminate the risks related to ICT completely. It is therefore essential, through good educational provision, to build pupils' resilience of the risks to which they may be exposed, so that they have the confidence and skills to face them and deal with them appropriately.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school relating to Online Safety:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about Online Safety and related incidents. A member of the governing body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the head teacher and / or ICT co-ordinator;
- Sitting on the school's Online Safety Committee (OSCOM);
- Reporting to relevant governors' meetings when necessary.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the ICT co-ordinator;
- The Headteacher and other senior leaders are responsible for ensuring that the ICT co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles - and to train other colleagues;
- The Headteacher and other senior leaders will ensure that there is a system in place to allow for the effective monitoring of internet use;
- The Headteacher and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

ICT Co-ordinator:

- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety Policy;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place – including logging the incident on CPOMS;
- Provides training and advice for staff;
- Liaises with the Local Authority where required;
- Sits on the school's Online Safety Committee (OSCOM);
- Attends relevant meetings of governors periodically;
- Reports to Senior Leadership Team;
- Ensures that users may only access the school's networks through secure, password protected log-ins;
- Takes a lead role in designing the programme of study for Online Safety;
- Provides education and information for parents/carers regarding Online Safety for their children.

Designated Person for Child Protection

Should be trained in Online Safety issues and be aware of the potential for child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate online contact with adults/strangers;
- Incidents of grooming;
- Cyber-bullying.

Teaching and Support Staff
Are responsible for ensuring that:

- They have awareness of Online Safety matters and the current school Online Safety policy;
- They have read, understood and signed the school staff Acceptable Use Policy (AUP);
- They report any suspected ICT misuse to the Headteacher or ICT co-ordinator in a timely manner;
- Digital communications with pupils are kept entirely professional;
- Online Safety issues are embedded within the curriculum and other school activities;
- Pupils understand and follow the school Online Safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They understand their responsibilities relating to their personal use of social media, as laid out in the Social Media Guidance for school staff document;
- They are aware that any incidents relating to cyber-bullying or Online Safety that occur out of school, will be acted upon by the school;
- In the event of being made aware of a 'sharing of nudes and semi-nudes' type incident (formerly known as 'sexting', they inform a Designated Safeguard Lead of the incident in a timely manner, record relevant details on CPOMS, and refer to UKCCIS guidance on sexting and peer on peer abuse as necessary;
- They are aware of Online Safety issues related to the use of mobile phones, wearable technologies, cameras and hand held devices, and that they monitor their use and implement current school policies with regard to these devices.

Pupils:

- Are responsible for using the school ICT systems in accordance with the pupil Acceptable Use Agreement, which they will be expected to sign before being given access to school systems;
- Will understand that incidents relating to cyber-bullying and/or Online Safety that occur out of school, will be investigated and acted upon in school;
- Pupils will be educated about the benefits and the risks associated with social media, and will be taught strategies to remain safe when online or accessing social media;
- Will be taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know, through the pupil Acceptable Use Agreement, school protocol on the use of mobile phones, digital and hand held devices. They should also know and understand school protocol on the taking / use of images, and on cyber-bullying;
- Will not use their personal mobile phones/devices on the school site, and must hand in any such technology to the school office by 9.00am each morning for safe keeping;
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school, and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Pupils from Years 1 to 6 will be given their own passwords, and this will be their only means of accessing school computer systems and the internet. They will be taught the importance of password security, and will keep their personal password private.

Parents / Carers
Parents / carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that parents and carers are often less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand relevant issues through parents' evenings, newsletters, letters, the school website, our

school X (formally Twitter) feed and by providing information about national or local Online Safety campaigns and/or literature.

The Head teacher and the ICT co-ordinator will ensure that the school's newsletter will indicate to parents where policies and advice relating to Online Safety are being added to or amended where appropriate, this information will also be shared on twitter. In this way parents can request paper copies if they have limited access to technology at home.

Our school actively encourages parent/carers to contact our school to discuss any Online Safety issues or concerns with the Headteacher, ICT co-ordinator or class teacher.

Use of Social Media

Social media websites are being used increasingly to fuel campaigns and complaints against schools, Headteachers, school staff, parents and pupils. Stivichall Primary School considers the use of social media websites in this way as unacceptable, and not in the best interests of the children or the whole school community. Any concerns must be made through the appropriate channels by speaking to the Class Teacher, the Headteacher or the Chair of Governors, so that they can be dealt with fairly, appropriately and effectively. The school's complaints procedure is available online, via the school website.

In the event that any pupil or parent/carer of a child being educated at Stivichall is found to be posting libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this. The school will also expect that any parent/carer or pupil removes such comments immediately. In serious cases the school will also consider its legal options to deal with any such misuse of social networking and other sites.

Additionally, and perhaps more importantly, is the issue of cyber bullying. In the event of any member of the school community using social media to publicly humiliate another by inappropriate social network entry, we will deal with this as a serious incident of bullying.

Guidance for Using Virtual / Video Conferencing

Video conferencing platforms can be an invaluable tool. However, all staff must be aware that a heightened sense of urgency can also lead to an increased risk regarding safeguarding and data protection. The following section is designed to make explicit the expectations in place when using virtual conferencing and online learning platforms.

- As a school, we used Seesaw as the online platform for communicating with children who were working from home during the pandemic. This platform is now used as appropriate for sending messages home, setting homework and is ready for use for home schooling if needed in the future.
- Microsoft Teams meetings should only be used where necessary in order to deliver small group sessions or 1-1 support from specialist staff. During a lockdown situation, the Teams meetings can be used to host live sessions with classes and groups of children in order to maintain effective communication and wellbeing.
- All Microsoft teams meetings with children must be approved by the Designated Safeguarding Lead.
- As a school, we must inform parents and carers of the sites that pupils/students are being asked to use, what they will be asked to do online and which members of staff they will be interacting with. During Lockdown, this has been Microsoft teams meetings, Zoom meetings and Seesaw.
- Parents evenings are completed using the school cloud and are set up in school by the digital advocate.

If the need to work remotely arises, we must consider the following safeguarding issues:

- It is not appropriate for staff members to hold one-to-one video conferences with a pupil/student. The staff Code of Conduct sets out expectations for behaviour.

- Staff, parents and pupils/students should be provided with acceptable use guidance.
- Two members of staff should be present for video calls to an individual child. This is to safeguard pupils/students and members of staff. When meetings are set up for groups of children, one member of staff can host the meeting. Settings to ensure pupils joining a meeting are kept in the lobby to avoid 1-1 interaction.
- The child should be notified if there is another adult present for the call.
- Parents/carers must be notified about the use of video conferencing and the school policy should be available to parents and carers. Behavioural expectations in line with the school policy for both Parents/Carers and members of staff must be followed.
- Video conferencing is to be used by adults working with groups of children. Where concerns arise, these should be flagged immediately using CPOMS as per safeguarding policy. If follow up communication is required, this should be completed using appropriate channels e.g. telephone conversation, online meeting etc.
- School safeguarding policies must be adhered to in the event of a child seeking to make a disclosure or remote abuse.
- Pupils/students should be reminded of reporting routes and how to seek help if they need to.
- Staff should separate their remote learning account from their personal online profiles and use a duplicate of the staff notice image or school logo for the platform profile picture. You should set up school accounts for any online platforms you use and check the privacy settings.

- When making telephone calls to parents/carers, either the school landline number or the dedicated school mobile telephone should be used for the purpose of communications.
- Never share any personal information e.g. personal telephone number, email accounts, Facebook and other social media links. Staff should never use personal social media accounts as a 'short cut' to communicate with parents and pupils. Further guidance on social media is covered in the social media guidance policy.
- For the purposes of video-conferencing, children should be sent links to zoom meetings using the secure platform of Seesaw. When using Teams, the children should access using their school login and have access to both the class general team and group teams with up to 6 members for live sessions.
- Use parents' or carers' email addresses or phone numbers to communicate with pupils/students individually, unless this poses a safeguarding issue. If staff need to communicate with pupils/students using the pupil/student's personal email address, another relevant member of staff should be copied into all emails.
- In the event of video conferencing, staff members are to work against a neutral background. Staff should present themselves as they would if they were giving a face-to-face lesson, in dress and in manner.
- Where lessons are delivered to a class, parents/carers and pupils should be provided with safeguarding and etiquette guidance in advance of the lesson. For example, the pupil/student must take lessons in a room with an open door. Parents should be notified of the timetable for their child in advance of the lessons taking place
- All staff to be aware of their setting's safeguarding and child protection policy and procedures.
- All staff members can contact the Designated Safeguarding Lead (DSL) or, in the event of the DSL being unavailable, deputy DSL, should they have any concerns about a child. Examples of potential concerns may include;
    - a staff member seeing, or hearing, something of concern during communication with a student
    - a disclosure, made by a pupil/student, when in communication with them during a phone call, via email or when video-conferencing.

- When making contact directly with pupils/students, as a means of checking on their welfare, schools should consider which methods are most appropriate for each pupil/student.
- Contact with pupils/students should happen within normal school hours.
- Schools should not record online lessons which include pupils without parental permission, or student permission where they have competency to consent.
- When sharing children's work with a class (on Seesaw), the child's permission must be sought first.

Online Safety – Preventing Radicalisation

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content.

Where staff, children or visitors find unblocked extremist content, they must report it to a member of the Safeguarding Team, School Leadership Team or ICT co-ordinator immediately.

Pupils and staff should know how to report internet content that is inappropriate or of concern. Children must be given online safety education each year and have regular reminders of the use of CEOPs and online safety links on the school website.

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach when using ICT. The education of pupils in Online Safety at Stivichall is therefore a vital part of the school's ICT provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience, and Online Safety education will be provided in the following ways:

- A planned and age-appropriate Online Safety scheme of work will be provided for each year group and must be taught annually; this is to be delivered alongside other opportunities including Safer Internet Week, Protective Behaviours, Jigsaw (PSHE sessions) and as part of our embedded curriculum where appropriate.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies;
- Pupils will be taught about the benefits and the risks associated with social media, and will be taught strategies to remain safe when online or accessing social media;
- The school will participate in Safer Internet Day which is organised nationally on an annual basis. These days also serve to refresh, update and remind pupils of the issues that they face every day of the year;
- Pupils will be taught across all subjects to be critically aware of the materials / content that they access online, and be guided to validate the accuracy of information;
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed via the internet;
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Rules for the use of ICT systems / internet will be displayed prior to children logging onto school systems;
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents / Carers

Many parents and carers have a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet, and can often be unsure about what they should do about it. "There is a generational digital divide". (Byron Report).

The school will, therefore, seek to provide information and pass on awareness to parents and carers through letters, the school newsletter, the school website and its Twitter feed.

Education & Training – Staff

It is essential that all adults working with children at Stivichall receive necessary Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff with network access should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy, Acceptable Use Policy and iPad User Policy;
- Online Safety training / CPD will be made available to staff as and when necessary;

- Staff will be given training to help them understand the issues of radicalisation, and are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns. This information also forms part of induction safeguarding training. Staff are updated as necessary in weekly staff meetings;
- The ICT co-ordinator will be able to attend training sessions and review guidance documents as appropriate;
- This Online Safety policy will be presented to, and discussed by staff in a staff meeting or INSET day;
- The ICT co-ordinator or members of the Senior Leadership Team will provide advice / guidance / training as required to individuals.

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with this being particularly important for those who are involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways, including: attendance at training provided by the Local Authority, National Governors Association or other relevant organisation; participation in school based training / information sessions for staff or parents.

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- All users will have clearly defined access rights to school ICT systems;
- All users will be provided with a username and password for the school network. This includes teachers, teaching assistants, other designated staff and all pupils in key stages 1 and 2. A central record of all passwords used on the school systems will be kept;
- The school is currently using a filtering service provided by Impero. This blocks any sites containing banned words or which come under predetermined categories. Any attempts to access such sites, or the typing of unacceptable words, triggers a screen shot which is sent to a central log. These are then checked by the ICT co-ordinator. Where such screen shots require a follow up investigation, the Headteacher will be informed;
- Requests from staff for websites to be removed from the filtered list will be considered by the ICT co-ordinator and members of the SLT. The removal, if approved, will be completed by the school IT support staff;
- The Headteacher and the ICT co-ordinator can monitor the activity of users on the school ICT systems, and users are made aware of this in the Acceptable Use Policy;
- Staff are forbidden from installing programmes on school workstations / portable devices without written permission from the ICT Co-ordinator or Headteacher (any such installation requires administrator login;
- The school infrastructure and individual workstations are protected by up to date virus software;
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured;
- As per the Acceptable Use Policy, users may only store pupil and sensitive data on the school server,

Microsoft Sharepoint, or on encrypted memory sticks that are provided by school.

Our Stivichall Curriculum

Online Safety should be a focus in all areas of the curriculum, and all staff should reinforce Online Safety messages in the use of ICT across the curriculum:

- Where pupils are allowed to freely search the internet (e.g. when using search engines) staff should be vigilant in monitoring the content of the websites that young people visit (the school recommended search engine is swiggle.org.uk;
- Pupils should be made aware that their activities when using school systems can be monitored and recorded, and encouraged / taught to act responsibly when using ICT;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a

situation, staff can request that the ICT co-ordinator or Headteacher temporarily removes specific websites from the filtered list for the period of study. Any request to do so, should be presented with clear reasons for the need;

- Pupils should be taught by all staff in all salient lessons to be critically aware of the materials / content that they access online, and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Acorns Wrap Around (after school club)

Our after school provision club (Acorns) use iPads that are separate from the curriculum iPads available during school time. Acorns staff monitor these devices, and staff teach pupils to respect the devices and use them in line with our school acceptable usage policy. Acorns staff deal with any instances whereby the devices are used inappropriately (in line with our online safety policy and social media guidance policy).

Consent and Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing / posting digital images on the internet. Those images may remain available on the internet forever, and in some cases cause harm or embarrassment to individuals in the short or longer term. 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 pupils 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 (such as on social networking sites);
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images;
- Staff will not publish any digital images of themselves or any other staff engaged in school activities on the personal pages of social networking sites;
- Staff will not publish any digital images of pupils engaged in school activities on the personal pages of social networking sites;
- Staff will ensure that their personal networking use is restricted, so that it is not publicly available;
- Staff will ensure that at all times their use of social media remains professional and does not bring the school into disrepute. This includes, but is not exclusive to, ensuring that pupils of the school do not have access to their personal sites unless there are good personal reasons that the Headteacher is aware of;
- Care should be taken when taking digital / video images of pupils, to ensure that they are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils must not take, use, share, publish or distribute images of other pupils or staff without their permission;
- Photographs published on the website, X, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school website or X account. These permissions are obtained each year and must be updated on the school Sharepoint site immediately. Staff must be aware of this and not publish images of pupils online where permission has been denied.

Data Protection and GDPR

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

The act states: Under the regulations, it's essential that the data you hold is '**processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**'.

Staff must ensure that:

- They take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- They use personal / sensitive data only on secure password protected computers and other devices;
- Personal / sensitive data is only moved or transported using secure encrypted memory sticks;
- They do not store personal or sensitive data on any non-encrypted USB stick or other device.

Escalating Security Incidents e.g. remote hack, password breach

In the event of a security breach the following protocol must be adhered to:

- Report immediately to the Head teacher, on-site technician and SLT.
- Isolate and quarantine affected machine(s) – support from technician both on-site and offsite (NS Optimum 01926 745608)
- If security incident occurs on an admin machine refer to Coventry City Council immediately (IT Service Desk 02476 786620)
- Log all incidents with Online Safety Lead including solution

Responding to Incidents of Misuse

It is expected that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible misuse of ICT. 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 such as:

- Child sexual abuse images;
- Criminally racist material;
- Criminal conduct, activity or materials.

The head teacher must be consulted with the evidence of the activity. If the evidence confirms the misuse the Headteacher has a duty to report the incident to the police.

As per safeguarding guidance – staff should not view images or videos on pupil's personal devices (see extra advice in UKCISS document, Sexting in schools and colleges).

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. The investigation should be conducted by the ICT co-ordinator and the Headteacher or other member of the SLT.

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.