ST JAMES
C.E. PRIMARY SCHOOL

DREAM • BELIEVE • LEARN • ACHIEVE

ONLINE SAFETY POLICY

This policy outlines our purpose in providing e-mail and access to the Internet at St James Primary and explains how the school is seeking to avoid the potential problems that unrestricted Internet access could give rise to.

INTERNET ACCESS IN SCHOOL

Providing access to the Internet in school will raise educational standards and support the professional work of staff.

Teachers will have access to the Internet offering educational resources, news and current events they will also be able to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LEA and DCSF. The Internet is being used to enhance the school's management information and business administration systems.

Pupils will have access to the Internet offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet will be provided with the Acceptable User Policy and will have its importance explained to them. Parents will be drawn to the Policy by letter and online within the Online Safety section of the schools' Website.

ROLES AND RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online incidents and monitoring reports. The Governor with responsibility for safeguarding will lead this role.

Governors will be encouraged to ensure that they have the skills and knowledge required to support the work of the Standards Committee in this area. They will be made aware of opportunities for relevant training e.g. attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation or participation in school training / information sessions for staff or parents.

Principal and Senior Leaders:
(Computing Subject Leader: Mrs Sara Pandor/Safeguarding Lead: Mrs Lisa Belfield)

- The Principal has a duty of care for ensuring the safety (including online) of members of the school community.
- The Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.
- The Principal is responsible for ensuring that staff receive suitable training to enable them to carry out their role and safeguard pupils.
- Takes day to day responsibility for online issues and has a leading role in establishing and reviewing the school online policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.

- Provides training and advice for staff.
- Liaises with the Local Authority / relevant body.
- Liaises with school technical staff.
- Receives reports of online incidents and creates a log of incidents to inform future online developments.
- Meets with Safeguarding Governor to discuss current issues.
- Reports regularly to Senior Leadership Team. Any incidents that are a Child Protection issue will be dealt with by the Designated Safeguarding Lead.

Network Manager / Technical staff:
'Computeam' are 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 technical requirements and any Local Authority / other relevant body Online Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant.
- That the use of the network /Internet /remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal.

Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of online matters and of the current online policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the Principal for investigation.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using agreed school systems.
- Online issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the online and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices. In lessons where Internet use is pre-planned, pupils should be guided to appropriate sites and they should be aware of what action to take if inappropriate material is found.

Child Protection / Designated Safeguarding Leads:

Should be trained in online issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Students/Pupils:

- Are responsible for using the school's digital technology systems in accordance with the Student / Pupil Acceptable User Policy.
- 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 and understand policies on the use of mobile devices and digital cameras.
- They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school (where appropriate)

POLICY STATEMENTS – EDUCATION AND 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 provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided and should be regularly revisited within the curriculum and assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line 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.
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Policy (AUPs) and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the Internet and mobile devices.
- In lessons where Internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

USING E-MAIL

All staff are strongly advised **NOT** to use or share their personal email account for school and therefore are issued with their own professional email which they will use appropriately to communicate with colleagues and schools' external services.

Pupils will learn how to use an e-mail application

- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed through consent letters that pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future IT developments by newsletters and the school website.

Online Safety will be taught to all pupils from EYFS and will be readdressed every year. Sessions will be taught using age appropriate resources and cover the following areas: Email, SMS Messaging, Social Networking and Cyber Bullying. All children within these sessions will have the opportunity to agree to their own Acceptable Users Policy.

If a reported incident arises outside of school, staff will log the event with the computing lead and/or learning mentors who will contact parents to arrange discussions with those necessary.

SOCIAL MEDIA – PROTECTING PROFESSIONAL IDENTITY

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, Risk assessment, including legal risk
- School staff should ensure that no reference should be made in social media to pupils, parents / carers or school staff. They do not engage in online discussion on personal matters relating to members of the school community. Personal opinions should not be attributed to the school or local authority

UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber- bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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.

USING INFORMATION FROM THE INTERNET

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true;
- When copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

MONITORING/REPORTING

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels:

- Staff will log the event with the Computing Lead.
- Contact will be made with the parents to inform.
- Discussion to take place with all parties. Serious incidents within school will be referred to the Child Protection Officer in consultation with Principal and the pupil's class teacher.
- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet by failing to follow the rules they have been taught and rules set within the acceptable users' policy; then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers and access to the Internet may be denied for a period.

MAINTAINING THE SECURITY AND SAFETY OF THE SCHOOL NETWORK

- We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons. As part of the IT SLA agreement the school receives regular Sophos Anti-Virus software updates. However it is the schools duty to notify the LA if there is a possible virus risk.
- Our internet access is purchased Computeam and the school has a "fileserver" which acts as the schools server, this provides a service designed for pupils including a "firewall" filtering system intended to prevent access to material inappropriate for children.
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan.
- Staff to ensure that when searching the Internet for images all projectors and Smartboards to be turned off, enabling a wider use of images banks.
- If staff or pupils discover unsuitable sites the IT co-ordinator will be informed. The URL (address) and content will be reported to the support team.

- If it is thought that the material is illegal, after consultation with Computeam, the site will be referred to the Internet Watch Foundation and the police.
- Our Rules for Responsible Internet Use will be posted near computer systems.
- The Principal will ensure that the policy is implemented effectively. All staff have been trained how to back-up their files using secure, encrypted remote access to the server.
- It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Computeam can accept liability for the material accessed, or any consequences thereof. A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Review Date: September 2018
Next review: September 2022