Local Arrangements for Online Safety at Ipsley C of E Middle School

(to be read in conjunction with CRST Online Safety Policy)

Rationale

The purpose of this document is to support the Central Region Schools Trust online safety policy.

It will aim to:

• set out the key principles expected of all members of our school community with respect to the use of computing and ICT-based technologies;

• safeguard and protect our children and staff;

• assist our school staff when working with children, to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;

• set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;

• have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies;

• ensure that all members of our school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;

• minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

• Exposure to illegal, inappropriate or harmful content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse

• Lifestyle websites, for example pro-anorexia/self-harm/suicide sites

• Hate sites

• Content validation: how to check authenticity and accuracy of online content

Contact

• Grooming

• Cyber-bullying in all forms

• Identity theft and sharing passwords

Conduct

• Privacy issues, including disclosure of personal information

• Digital footprint and online reputation

• Health and well-being (amount of time spent online (Internet or gaming)

• Child on Child abuse including sexting (sending and receiving of personally intimate images also referred to as self-generated indecent images/youth produced sexual imagery)

• Copyright (care or consideration for intellectual property and ownership - such as music and film)

Commerce

- Online gambling
- Inappropriate advertising

- Phishing or financial scams

Education and curriculum

School online safety curriculum

This school has a clear, progressive online safety education programme as part of the computing curriculum and also the PSHE/Learning for Life curriculum. This covers a range of skills and behaviours appropriate to their age and through this aims to:

• plan careful Internet and device use to ensure that it is age-appropriate, safe and supports the learning objectives for specific curriculum areas;

• teach pupils about their responsibilities through an end-user acceptable use policy (AUP);

• ensure staff model safe and responsible behaviour in their own use of technology during lessons;

• ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

• ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

Staff and governor training

Ipsley C of E Middle School:

• ensures staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

• makes regular training available to staff on online safety issues and the school's online safety education program;

• provides all new staff (including those on university/college placement and work experience) with information and guidance on the online safety policy and the school's acceptable use policy (AUP).

Parent awareness and training

Ipsley C of E Middle School provides a programme of advice, guidance and training for parents, including:

• information leaflets, in-school newsletters, information and advice on the school website;

• suggestions for safe Internet use at home;

• provision of information about national support sites for parents.

Expected conduct and incident management

Expected conduct

At Ipsley C of E Middle School, all users:

• are responsible for using the school systems in accordance with the relevant school policies;

• need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

• 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;

• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and/or use of images and on cyber-bullying.

Staff are responsible for reading both the school's Trust Online Safety Policy, the local arrangements for online safety document, and using the school computing systems accordingly, including the use of mobile phones, and hand held devices.

Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/carers should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident management

In this school and in line with the Central Region Schools Trust Online Safety Policy:

• there is strict monitoring (through the use of our online monitoring software 'SENSO'), application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions

• all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

• support is actively sought from other agencies as needed (e.g. the Local Authority)

• monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders and governors

• parents/carers are informed of online safety incidents involving pupils for whom they are responsible. Where possible, this would happen on the day of the incident as it is a crucial part of our safeguarding process.

• Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Password policy

• At Ipsley C of E Middle School, we make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;

• All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

• All pupils have their own unique username and passwords.

Social networking

School staff will ensure that in private use:

• 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 the school community

• personal opinions should not be attributed to the school or Trust

• they ensure their use of social networking sites is respectable and appropriate at all times

• personal profiles do not identify their place of work

• they do not use a work email to sign up to non-work related web-accounts

• they do not have contact with pupils using social media

• they do not add pupils as friends or respond to friend requests from pupils

• secure and suitable strength passwords are used

• security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content

Personal mobile phones and mobile devices

• Mobile phones brought into school are entirely at the staff member, pupils', parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

• Pupil mobile phones can be brought into school, but are handed in to the class teacher/tutor during the day for all pupils. All staff and visitors are requested to keep their phones on silent and use them only during break times in staff work rooms and outside of the school premises.

• The recording, taking and sharing of images, video and audio on any mobile phone by any member of the school community is to be avoided; except where it has been explicitly agreed otherwise by the Principal (see bullet point below regarding photos/videos containing pupils). Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

• Staff and visitors should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.

• The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Staff use of devices

• Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

• Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional or personal capacity, unless using the school supplied app 3CX.

• Staff will use a school phone or 3CX where contact with pupils, parents or carers is required.

• If a member of staff breaches the school policy then disciplinary action may be taken. Staff members may be required to use a mobile phone for school duties, for instance in case of emergency during off-site activities.

Digital images and video

In this school:

• We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

• We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

• The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;

• Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;

• Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

• Pupils are taught that they should not post images or videos of others without their permission.

We teach pupils about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

These Local Arrangements will be reviewed in a timely manner in accordance with the Central Region Schools Trust Online Safety Policy.

Appendix A

Key Responsibilities

Principal/DSL

• To take overall responsibility for online safety provision.

• To take overall responsibility for data and data security.

• To ensure the school uses an approved, filtered Internet service, which complies with current statutory requirements.

• To be responsible for ensuring that all teaching and non-teaching staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant.

• To be aware of procedures to be followed in the event of a serious online safety incident.

• To receive regular monitoring reports from the online safety lead.

• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures.

Online safety lead/DDSL

• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

• To promote an awareness and commitment to online safeguarding throughout the school community.

• To ensure that online safety education is embedded across the curriculum.

• To liaise with School technical staff on the latest developments.

• To communicate regularly with SLT and the designated online safety governor / governing body committee to discuss current issues, review incident logs and filtering.

• 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 online safety is continually monitored via SENSO.

• To facilitate training and advice for all staff.

• To liaise with the local authority (LA) and other relevant agencies.

• To be regularly updated regarding online safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media.

• To oversee the delivery of the online safety element of the computing curriculum.

• To liaise with the PSHE lead on a regular basis

Governors

• To ensure that the school follows all current online safety advice to keep the children and staff safe.

• To approve the 'Local Arrangements for Online Safety' document and review the effectiveness of this.

• To support the school in encouraging parents and the wider community to become engaged in online safety activities.

Network manager /technician

• To report any online safety related issues that arises, to the online safety lead.

• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.

• To ensure that provision exists for misuse detection and malicious attack eg keeping virus protection up to date.

• To ensure the security of the school computer system.

• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.

• To ensure the school's policy on web filtering is applied and updated on a regular basis.

• To ensure that he/she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

• To ensure that the use of the network / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse / attempted misuse can be reported to the online safety lead/SLT for investigation / action / sanction .

• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

• To keep up-to-date documentation of the school's e-security and technical procedures

Teachers

• To embed online safety issues in all aspects of the curriculum and other school activities.

• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).

• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

All staff

• To read, understand and help promote the Central Region Schools Trust Online Safety Policy and the Local Arrangements for Online Safety document.

• To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

• To report any suspected misuse or problem to the e-safety lead.

• To maintain an awareness of current online safety issues and guidance e.g. through CPD.

• To model safe, responsible and professional 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 (ePraise), and never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils

• Read, understand and adhere to the pupil acceptable use policy.

• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• Understand the importance of reporting abuse, misuse or access to inappropriate materials.

• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.

• To know and understand school arrangements on the use of mobile phones, digital cameras and hand held devices.

• To know and understand school arrangements on the taking / use of images and on cyber-bullying.

• To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Local Arrangements for Online Safety document covers their actions out of school, if related to their membership of the school.

• 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 help the school in the creation/ review of online safety documents.

Parents/carers

• To support the school in promoting online safety

• To read, understand and promote the school pupil acceptable use agreement with their children.

• To access the school website / on-line pupil records in accordance with the relevant school acceptable use policy.

• To consult with the school if they have any concerns about their children's use of technology.

External groups

• Any external individual / organisation will be made aware of the school's acceptable use policy (AUP) prior to using any equipment or the internet within school.

Appendix B

Pupil Acceptable Use Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to use all digital technologies safely at all times.

This Acceptable Use Agreement is intended to ensure:

- pupils will be responsible users and stay safe while using the internet and other digital technologies.
- school systems are protected from accidental or deliberate misuse that could put the security of the systems at risk.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure. I will not share it, nor will I try to use any other person's username and password.
- I will not disclose contact details, inappropriate personal details or images or share any other personal information about myself or others when online.
- I will never arrange to meet anyone I have communicated with online.
- I will immediately report any unpleasant or inappropriate material, messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting, unless I have permission from a member of staff to do so.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not use any digital platform to bully, harass, offend or insult others.
- I will not create, access or distribute any material that may cause offence, including images of staff, pupils, parents or governors.
- I will only use social media sites with staff permission.

I recognise that the academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones, USB devices, etc.) in school if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement in the same way as if I was using school equipment.
- I will not try to bypass the filtering/security systems in place.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install, attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will not eat or drink near computer equipment.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspension or exclusion, contact with parents/carers and in the event of illegal activities involvement of the police.