Becton School
Together We Can

# Online Safety Policy

November 2018
To be reviewed November 2019

Content

**Background / Rationale**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and *students* learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Loss of privacy / control of personal information
- Grooming or exploitation by people who they make contact with on the internet.
- The sharing / distribution of personal images and personal information without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video / internet games
- Being unable to judge the accuracy, relevance and whether the information is from a reliable source.
- Plagiarism (copying a piece of written work or an idea and claiming it as your own) and breach of copyright (the illegal copying or use of creative work e.g. music, video, photographs, documents etc. without the owners consent)
- Illegal downloading of music or video files
- Hacking into personal profiles, ineffective system security and viruses (giving access to personal and financial information)
- The potential for excessive use which may impact on the social and emotional development and learning of the child or young person.

Many of these risks reflect situations in the off-line world and it is essential that this Online Safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents /

carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Safeguarding working group made up of:

- Sacha Schofield,
- Sarah Robinson
- Eddy Hartley

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

- Staff meetings
- Governors meeting
- School website

Schedule for Development / Monitoring / Review

| | |
|---|---|
| This Online Safety policy was approved by the *Governing Body / Governors Sub Committee on:* | November 2018 |
| The implementation of this Online Safety policy will be monitored by the: | Mel Kilner - Online Safety Coordinator |
| Monitoring will take place at regular intervals: | Annually |
| The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals: | Annually |
| The Online Safety 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 Safety or incidents that have taken place. The next anticipated review date will be: | *November 2018* |
| Should serious Online Safety incidents take place, the following external persons / agencies should be informed: | James Gibson – DSL |

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
- *students (including Every Child Matters Survey)*

- parents / carers
- staff

**Scope of the Policy**

This policy applies to all members of the school community (including staff, students, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevent 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 school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

**Roles and Responsibilities**

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school.
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 Online Safety Co-ordinator / Officer.
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles..
- The Headteacher and another member of the Senior Leadership Team / Senior Management 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. (see flow chart on dealing with Online Safety incidents – included in a later section –and relevant Local Authority HR / disciplinary procedures)

**Online Safety Coordinator / Officer:**

- leads the Online Safety committee
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

**Network Manager / Technical staff:**

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements and any relevant Local Authority policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he keeps up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff
are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation / action / sanction
- digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school Online Safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are 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
- in lessons where internet use is pre-planned students 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

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

This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the school. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the school.

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, 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 and young people for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child/young person, 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/young person 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 and young people in their care (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the school into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

**Wider personal use of digital communications:**

Everyone should be able to enjoy the benefits of digital technologies. Staff and volunteers should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as “friends” on social networking profiles and which information / photos are available to those friends
- Privacy settings should be frequently reviewed.
- Creating different ‘groups of friends’ should be considered to control what and how much information ‘friends’ can see.
- The amount of personal information visible to those on “friends” lists should be carefully managed and users should be aware that “friends” may still reveal or share this information.
- “Digital footprint” – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them

- A large proportion of employers engage in searches of the internet when selecting candidates and are influenced by the content they find.

**Designated person for child protection / Designated Safeguarding Lead should be trained in Online Safety issues 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

**Online Safety Committee/Team**

Members of the Safeguarding Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety policy / documents.

**Students:**

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 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 / use of images and on cyber-bullying.
- 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

**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 ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local Online Safety campaigns / literature.* Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

**Community Users**
Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

**Policy Statements**

**Education – students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* 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 will be provided in the following ways:

- A planned and progressive Online Safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students 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
- Students should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

**Education – parents / carers**

Many parents and carers have only 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 the children's on-line 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 are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website, VLE
- Reference to the Sheffield Safeguarding website and other relevant resources.

**Education & Training – Staff**

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 will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.

- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at SSCB / other information / training sessions and by reviewing guidance documents released by UKKCIS/ other relevant research .
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training as required to individuals as required

**Training – Governors**

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the school / National Governors Association / SSCB or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be 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 need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements and Acceptable Usage Policy and any relevant Local Authority policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
- All users at KS2 and above will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, 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.
- The school maintains and supports the managed filtering service provided by YHGfL.
- Any filtering issues should be reported immediately to YHGfL
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and logged by YHGfL.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate communication system is in place for users to report any actual / potential Online Safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The Network Manager has restricted the downloading of executable files by users and has prevented staff from installing programmes on school workstations / portable devices.

- The Network Manager has restricted access to removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- 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.

**Curriculum**

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

- in lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, eg using search engines, 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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.
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

**Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students 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 students 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 eg 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year)

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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 must ensure that they:

- At all times take care 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.
- Transfer data using encryption and secure password protected devices.

Secure Transfer Process

All sensitive information or personal data sent by email or fax will be transferred using a secure method.

Do not include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

**Communications**
A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

| | Staff & other adults | | | | Students | | | |
|---|---|---|---|---|---|---|---|---|
| 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 | x | | | | | | X | |
| Use of mobile phones in lessons | | | | x | | | | x |
| Use of mobile phones in social time | x | | | | | | X | |
| Taking photos on mobile phones or other camera devices | | | | x | | | | x |
| Use of hand held devices eg PDAs, PSPs | x | | | | | | X | |
| Use of personal email addresses in school, or on school network | | x | | | | | X | |
| Use of school email for personal emails | | | | x | | | | x |
| Use of chat rooms / facilities | | | | x | | | | x |
| Use of instant messaging | | | | x | | | | x |
| Use of social networking sites | | | | x | | | | x |
| Use of blogs | | x | | | | | x | |

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- 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 students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students at KS2 and above will be provided with individual school email addresses for educational use.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**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** | | | | | X |
| | **promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation** | | | | | X |
| | **adult material that potentially breaches the Obscene Publications Act in the UK** | | | | | X |
| | **criminally racist material in UK** | | | | | X |
| | **pornography** | | | | x | |
| | **promotion of any kind of discrimination** | | | | x | |
| | **promotion of racial or religious hatred** | | | | x | |
| | **threatening behaviour, including promotion of physical violence or mental harm** | | | | x | |
| | **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** | | | | x | |
| **Using school systems to run a private business** | | | | | x | |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school** | | | | | x | |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** | | | | | x | |
| **Revealing or publicising confidential or proprietary information (eg** | | | | | x | |

| | | | | | |
|---|---|---|---|---|---|
| **financial / personal information, databases, computer / network access codes and passwords)** | | | | | |
| **Creating or propagating computer viruses or other harmful files** | | | | x | |
| **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** | | | | x | |
| **On-line gaming (educational)** | x | | | | |
| **On-line gaming (non educational)** | | x | | | |
| **On-line gambling** | | | | x | |
| **On-line shopping / commerce** | | x | | | |
| **File sharing** | | | | x | |
| **Use of social networking sites** | | | | x | |
| **Use of video broadcasting eg Youtube** | | | x | | |

**Responding to incidents of misuse**

It is hoped 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 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 ie.

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

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:

Students Actions / Sanctions

| Incidents: | Refer to class teacher / tutor | Refer to Deputy Head | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | | x | x | x | x | x | x | x |
| Unauthorised use of non-educational sites during lessons | x | | | | x | x | | x | |
| Unauthorised use of mobile phone / digital camera / other handheld device | x | | x | | x | x | | x | |
| Unauthorised use of social networking / instant messaging / personal email | x | | x | | x | x | | x | |
| Unauthorised downloading or uploading of files | x | | x | | x | x | | x | |
| Allowing others to access school network by sharing username and passwords | x | | x | | x | x | | x | |
| Attempting to access or accessing the school network, using another student's / pupil's account | x | | x | | x | x | x | x | |
| Attempting to access or accessing the school network, using the account of a member of staff | x | | x | | x | x | x | x | |
| Corrupting or destroying the data of other users | x | | x | | x | x | x | x | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | x | | x | x | x | x | x | x | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Continued infringements of the above, following previous warnings or sanctions | x | | x | x | x | x | x | x | x |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | x | | x | x | x | x | x | x | x |
| Using proxy sites or other means to subvert the school's filtering system | x | | x | | x | x | x | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | | x | | x | x | | x | |
| Deliberately accessing or trying to access offensive or pornographic material | | | x | x | x | x | x | x | x |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | x | | x | x | x | x | x | x | x |

Staff Actions / Sanctions

| Incidents: | Refer to line managerr | Refer to Headteacher | RRefer 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).** | | x | x | x | x | x | x | x |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | | x | x | | x | x | | |
| Unauthorised downloading or uploading of files | | x | x | | x | x | | |
| 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 | | x | x | | x | x | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | | x | x | | x | x | | |
| Deliberate actions to breach data protection or network security rules | | x | x | x | x | | x | x |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | x | x | x | x | | x | x |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | x | x | x | x | | x | x |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students | | x | x | | x | x | | |
| Actions which could compromise the staff member's professional standing | | x | x | x | x | x | x | |
| Actions which could bring the school | | x | x | x | x | x | x | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 | | x | x | | x | | x | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | x | x | | x | x | | |
| Deliberately accessing or trying to access offensive or pornographic material | | x | x | x | x | | x | x |
| Breaching copyright or licensing regulations | | x | x | | x | x | | |
| Continued infringements of the above, following previous warnings or sanctions | | x | x | x | x | | x | x |

Appendices

Student / Pupil Acceptable Usage Policy template
Staff and Volunteers Acceptable Usage Policy template
Parents / Carers Acceptable Usage Policy Agreement template
Use of Digital Images
School Personal Data Policy template
Flowchart for Response to an incident of Concern
School Online Safety Charter for Action
Ideas for schools to consider
Links to other organisations, documents and resources
Legislation

**Student / Pupil Acceptable Use Policy Agreement Template**

**School Policy**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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 safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *students* will have good access to ICT to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

**Acceptable Use Policy Agreement**

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

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password with anyone or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology to support our education:

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- 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 take or distribute images of anyone without their permission.

I understand that the school has a responsibility to keep the technology secure and safe:

- I will only use my personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use chat and social networking sites.

When using the internet for research for my school work, I understand 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 find is accurate, as I understand that the work of others may not be correct.

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

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this is cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the school network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.**

**Student / Pupil Acceptable Use Agreement Form**

This form relates to the student / pupil Acceptable Use Policy (AUP), which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

| | | |
|---|---|---|
| Name of Student / Pupil | | |
| Group / Class | | |
| Signed | | |

**Becton School**

**Acceptable Use Policy for Young Children**

**This is how we stay safe when we use computers:**

I will ask *a teacher / an adult* if I want to use the computer

I will only use activities that *the teacher /an adult* has told or allowed me to use.

I will take care of the computer and other equipment

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

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

I know that if I break the rules I might not be allowed to use a computer.

*Signed (child):……*

Signed (parent): ……..

# Think before you click

| | |
|---|---|
| S  | I will only use the Internet and email with an adult |
| A  | I will only click on icons and links when I know they are safe |
| F  | I will only send friendly and polite messages |
| E  | If I see something I don't like on a screen, I will always tell an adult |

My Name:

My Signature:

**Staff Acceptable Use Policy 2016**
**Guidance for Use**

Senior Leadership Teams (SLT) will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities in schools and settings. Nevertheless it is essential that the use of ICT and online tools is carefully managed to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated.
This template Acceptable Use Policy (AUP) provides a structure which is appropriate to the school Online Safety ethos and approach. The AUP will need to be adapted by the school for a variety of different audiences and for their individual requirements and systems. It should be developed by a member of SLT and must be approved by the Head Teacher and Governing Body. **It is recommended that staff should be actively involved in writing the AUP to ensure it is appropriate and meets the requirements of the establishment.**

***Legislation***

Schools may wish to read relevant legislation and information regarding this document and amend the school's AUP accordingly. Schools have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Schools may also wish to read and consider the document "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009), which contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

***Data Protection Act 1998***

Schools must also ensure they comply with the Data Protection Act (DPA) 1998. Under the DPA every organisation that processes personal information (personal data) must notify (register with) the Information Commissioner's Office, unless they are exempt. Specific guidance for education establishments, including information on how to register and check notification may be found here: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Schools should have a Data Protection and Security Policy in place to outline the legal responsibilities and actions taken to protect personal data in accordance with the DPA. This may include password safety, use of encryption, use of laptops, email and portable data storage devices (e.g. memory sticks) not sharing login information etc. Schools can read more information from the Information Commissioner's Office: http://www.ico.gov.uk/

A Staff AUP is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

In order to protect staff members it is essential to have an AUP in place which has been viewed and understood. All employees (including teaching and non-teaching staff) must be aware of the school rules for use of information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees (whether from Sheffield City Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

With internet use becoming more prominent in every day life for personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. It is therefore important that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements). It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis. All members of staff should read, understand and sign the AUP before being granted access to any of the schools' ICT systems.

***Social Media***

Some settings may wish to provide more explicit guidance for staff around use of social networking and email as, even when use of social media sites such as Facebook and Twitter occur in their own time using their own computer, it can leave staff vulnerable to abuse or a blurring of professional boundaries.

Schools must be aware they cannot ban staff from using sites in their own personal time; however they can put in place appropriate guidance and boundaries around staff interaction with pupils (past or present) and parents. It is recommended that any contact with pupils and parents only takes place via school approved communication channels e.g. school email address or the school learning platform so it can be monitored and traced in the case of an allegation or concern. However, schools must recognise that in some cases there may be pre-existing relationships which mean that any "ban" from adding pupils or parents as friends or contacts on personal social networking sites may be difficult to enforce. It is therefore recommended that members of staff are encouraged to make SLT aware of these exceptions in order to protect themselves from allegations or misinterpreted situations.

It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff should be advised to check their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared).

***Use of Equipment***

Settings may also wish to consider adding a statement regarding their policy on staff using school equipment for personal use. Occasional personal use of the school's computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However this is at the school's discretion and can be revoked at any time. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and any policies relating to staff conduct and personal use

must not interfere with the member of staff's duties or be for commercial purpose or gain (unless authorised by the SLT).

***Use of Personal Devices***

It is recommended that staff do not use their own devices for school business, such as personal mobile phones to communicate with pupils whilst on educational visits or using the camera/video on their mobile phone. On occasions when the use of a personal camera is necessary, permission should be sought from the Headteacher/SLT. The images should then be transferred to the school network and deleted from the camera.

Schools may also consider providing staff with a written process or chart to follow for reporting any incidents or concerns to ensure that all members of staff are aware of and understand the school's specific safeguarding procedures. **Where the school outsources any ICT services it is essential that an AUP is created as part of the service level agreement and is owned and enforced by both the managed service and the school.**

The Staff AUP should be reviewed regularly (at least annually) and should be revisited and updated in response to any changes, for example after an incident, introduction of new technologies or after any significant changes to the school organisation or technical infrastructure. Any amendments to the AUP should then be communicated to all staff.

The AUP template suggests a range of statements and should be used to develop the schools Online Safety ethos and whole-school approach. This AUP template is suitable for all schools and other educational settings (such as Pupil Referral Units, 14-19 settings and Hospital Schools etc) and we encourage establishments to ensure that their AUP is fit for purpose and individualised for their context. For simplicity we have used the terms 'school' and 'pupils', but wider educational settings are equally relevant.

If schools or settings wish to discuss the use and application of Acceptable Use Policies or any other Online Safety concerns, please contact the Online Safety Project Manager, Sheffield Safeguarding Children Board julia.codman@sheffield.gov.uk 0114 2736945 or contact the Safeguarding Advisory Service 0114 2053554

## Further Information

Sheffield Schools and settings can consult with the Online Safety Manager via: julia.codman@sheffield.gov.uk or telephone 0114 2736945.

Training is available via Safeguarding Training Service on 0114 Telephone: 0114 2735430 or email safeguardingchildrentraining@sheffield.gov.uk

The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around Online Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

"Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety

"Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx

Teach Today is a useful website which provides useful advice and guidance for staff from industry: http://en.teachtoday.eu

360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/

"Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

**Staff ICT Acceptable Use Policy 2016**

*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 Communication 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 ICT use should be consistent with the school ethos, other appropriate policies and the Law.

I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, 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 Data Protection Act 1988. 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. No personal student data may be removed from the school site (such as via email or on memory sticks or CDs). 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).. 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 ICT 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 Designated Child Protection Coordinator (Sacha Schofield) and/or the Online Safety Coordinator (Sacha Schofield) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Sacha Schofield) the Online Safety Coordinator or (Ed Hartley) the designated lead for filtering as soon as possible.

I will not attempt to bypass any filtering and/or security systems put in place by the school. 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 ICT Support Provider (Ed Hartley) as soon as possible.

My electronic communications with pupils, 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 ICT 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 ICT 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 pupils 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 practise online either in school or off site, then I will raise them with the Online Safety Coordinator (Sacha Schofield) or the 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 ~~i~~nformation 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 and agree to comply with the Staff ICT Acceptable Use Policy.**

Signed: ……..... Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

**Becton School**
**Parent / Carer Acceptable Use Policy Agreement**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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 safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

- **that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.**
- **that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.**
- **that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.**

The school will try to ensure that *students* will have good access to ICT to enhance their learning and will, in return, expect the *students* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

**Permission Form**

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's Online Safety.

Signed Date

**Use of Digital / Video Images**

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Parents are requested to sign [redacted] ake and use images of their children.

**Permission Form**

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *student / pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed Date

# School Personal Data Handling Policy

## Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

## Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

## Responsibilities

The school's Senior Risk Information Officer (SIRO) is Judith Bradshaw. They will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held and for what purpose
- how information as been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

**Registration**
The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

**Training & awareness**
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset

**Identification of data**
The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.
Secure Storage of and access to data
The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.
Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.
The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject

**Secure transfer of data and access out of school**
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

**Disposal of data**
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.
The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.
*A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

**Audit Logging / Reporting / Incident Handling**
As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.
The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.
The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading
Teachernet – Data processing and sharing -
**http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/**
Office of the Information Commissioner website:
**http://www.informationcommissioner.gov.uk**
Office of the Information Commissioner – guidance notes: Access to pupil's information held by schools in England

# Response to an Incident of Concern

**Online Safety Incident Occurs**

If a child is at immediate risk

Inform the Designated Child Protection Coordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Sheffield Police (999) urgently if there is immediate danger

**Contacts**

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

**Illegal Activity of Material found or suspected**

**Unsure**

**Inappropriate Activity or Material**

Content

Activity

Consult with Online Safety Project Manager

Activity

Content

Contact Online Safety Project Manager

Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police

Child

Staff

Child

Staff

Report to Filtering Manager and / or Schools Broadband Help Desk

Contact Safeguarding Advisory Desk for advice

Report to CEOP www.ceop.police.uk

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from Online Safety Officer

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from Online Safety Officer

**Review Schools Online Safety policies and procedures, record actions in Online Safety Incident log and implement any changes for future**

**Contact Details**

| |
|---|
| Schools Designated Child Protection Officer: Sacha Schofield |
| School Online Safety Coordinator: Sacha Schofield |
| Safeguarding Children Board Online Safety Manager: Diane Joynson |
| |

**Online Safety – A School Charter for Action**

| | |
|---|---|
| Name of School | Becton School |
| Name of Local Authority | Sheffield |

We are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential Online Safety risks.

Our school community

Discusses, monitors and reviews our Online Safety **policy** on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports **staff** in the use of ICT as an essential tool for enhancing learning and in the embedding of Online Safety across the whole school curriculum.

Ensures that **pupils** are aware, through Online Safety education, of the potential Online Safety risks associated with the use of ICT and mobile technologies, that all Online Safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's Online Safety policy.

Provides opportunities for **parents/carers** to receive Online Safety education and information, to enable them to support their children in developing good Online Safety behaviour. The school will report back to parents / carers regarding Online Safety concerns. Parents/carers in turn work with the school to uphold the Online Safety policy.

Seeks to learn from Online Safety good practice elsewhere and utilises the support of the **Sheffield Safeguarding Children Board and relevant organisations** when appropriate.

| | |
|---|---|
| Chair of Governors | Mr David Poulsom |
| Headteacher | |
| Pupil Representative | Sacha Schofield |
| | |

Ideas for schools to consider

Discuss, monitor and review

- Do we hold discussions on Online Safety and its definition, involving staff, children and young people, governors and parents?
- Do we keep a record of the incidence of Online Safety incidents, according to our agreed definition, and analyse it for patterns – people, places, groups, technologies?
- Do we ask ourselves what makes an e-safe school?
- What is our school doing to ensure that our children and young people do not feel vulnerable and are safe to learn, when engaged in online activities?
- Do we celebrate our successes and draw these to the attention of parents/carers and the wider community?

Support everyone in the school community to identify and respond

- Do we work with staff and outside agencies to identify all potential forms of Online Safety incidents?
- Do we actively provide systematic opportunities for developing pupils' skills to develop safe online behaviour?
- Have we considered all the opportunities where this can be addressed – through the curriculum; through corridor displays; through assemblies; through the School Council; through peer support; and through the website and parents' evenings and newsletters?
- Do we ensure that there is support for vulnerable children and young people?
- Do we train all staff to be aware of potential Online Safety issues and follow school policy and procedures on Online Safety?
- Do our staff feel adequately supported to be able to respond to and manage Online Safety related incidents?

Ensure that children and young people are aware of how and to whom Online Safety incidents should be reported and understand that all Online Safety concerns will be dealt with sensitively and effectively

- Do we acknowledge and learn from the high level of skills and knowledge of children and young people in the use of new technologies? (often referred to as the "digital natives")
- Do we regularly canvass children and young people's views on the extent and nature of Online Safety issues?
- Do we ensure that young people know how to express worries and anxieties about Online Safety?
- Do we ensure that all children and young people are aware of the range of sanctions which may be applied against those involved in Online Safety misuse?
- Do we involve children and young people in Online Safety campaigns in school?
- Do we demonstrate that we are aware of the power of peer support? Have we created and publicised schemes of peer mentoring or counselling; buddying or mediation, for example?

- Do we include the phone numbers of help-lines in the school's student planners?
- Have we made children and young people aware of "how to report abuse"?
- Do we have an Online Safety notice board?
- How else do we bring Online Safety messages to children and young people's attention?
- What role does our School Council already play in our Online Safety work? How might that involvement be enhanced?
- Do we offer sufficient support to children and young people who have been involved in Online Safety incidents?
- Do we work with children and young people who have been involved, or may be seen as being at risk?

Ensure that parents/carers are aware of Online Safety issues and that those expressing concerns have them taken seriously

- Do we work with parents and the local community to address issues beyond the school gates that give rise to Online Safety issues? – particularly with regard to the possible lack of filtering and monitoring of internet access by children and young people out of school and with regard to cyber-bullying incidents

- Do parents know whom to contact if they are worried about Online Safety issues?
- Do parents know about our complaints procedure and how to use it effectively?

Learn from effective Online Safety work elsewhere and establish effective collaboration

- Have we invited colleagues from a school with effective Online Safety policies and practice to talk to our staff?
- Have we involved the Sheffield Safeguarding Children Board staff or other local / regional experts in any way?
- Do we have an established link with the police?

Links to other organisations or documents

The following sites will be useful as general reference sites, many providing good links to other sites:

Sheffield Safeguarding Children Board http://www.safeguardingsheffieldchildren.org.uk
Safer Internet Centre: http://www.saferinternet.org.uk/

UK Council for Child Internet Safety: http://www.education.gov.uk/ukccis

CEOP - Think U Know - http://www.thinkuknow.co.uk/

Childnet - http://www.childnet.com

Netsmartz http://www.netsmartz.org/index.aspx

Teach Today http://www.teachtoday.eu/

Internet Watch Foundation – report criminal content: http://www.iwf.org.uk/

Byron Review ("Safer Children in a Digital World") http://webarchive.nationalarchives.gov.uk/tna/+/dcsf.gov.uk/byronreview/

Guidance for safer working practice for adults that work with children and young people - http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

Information Commissioners Office/education: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

ICO guidance on use of photos in schools: http://www.ico.gov.uk/youth/sitecore/content/Home/for_the_public/topic_specific_guides/schools/photos.aspx

Ofsted survey: http://www.ofsted.gov.uk/Ofsted-home/Publications-and-research/Browse-all-by/Documents-by-type/Thematic-reports/The-safe-use-of-new-technologies/(language)/eng-GB

Plymouth Early Years Online Safety Toolkit: http://www.plymouth.gov.uk/early_years_toolkit.pdf

Protecting your personal information online: http://www.ico.gov.uk/~/media/documents/library/data_protection/practical_application/protecting_your_personal_information_online.ashx

Getnetwise privacy guidance: http://privacy.getnetwise.org/

**Children and Parents**

Vodafone Parents Guide: http://parents.vodafone.com/

NSPCC: http://www.nspcc.org.uk/help-and-advice/for-parents-and-carers/internet-safety/internet-safety_wdh72864.html

Google guidance for parents: http://www.teachparentstech.org/

E-Parenting tutorials: http://media-awareness.ca/english/parents/internet/eparenting.cfm

Practical Participation – Tim Davies: http://www.practicalparticipation.co.uk/yes/

Digital Citizenship: http://www.digizen.org.uk/

Kent "Safer Practice with Technology": http://kentrustweb.org.uk/CS/community/kent_teachers/archive/2009/07/07/safer-practice-with-technology-for-school-staff.aspx

Connect Safely Parents Guide to Facebook: http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html

Ofcom – Help your children to manage the media: http://consumers.ofcom.org.uk/2010/10/parental-controls-help-your-children-manage-their-media/

Mobile broadband guidance: http://www.mobile-broadband.org.uk/guides/complete-resource-of-internet-safety-for-kids/

Orange Parents Guide to the Internet: http://www.orange.co.uk/communicate/safety/10948.htm

O2 Parents Guide: http://www.o2.co.uk/parents

FOSI – Family Online Internet Safety Contract: http://www.fosi.org/resources/257-fosi-safety-contract.html

Cybermentors (Beat Bullying): http://www.cybermentors.org.uk/

Teachernet Cyberbullying guidance: **http://www.digizen.org/resources/cyberbullying/overview**

"Safe to Learn – embedding anti-bullying work in schools" **http://www.anti-bullyingalliance.org.uk/tackling_bullying_behaviour/in_schools/law,_policy_and_guidance/safe_to_learn.aspx**

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

CBBC – stay safe: http://www.bbc.co.uk/cbbc/help/home/

**Technology**

Kaspersky – advice on keeping children safe - http://www.kaspersky.co.uk/keeping_children_safe

Kaspersky - password advice: www.kaspersky.co.uk/passwords

CEOP Report abuse button: http://www.ceop.police.uk/Safer-By-Design/Report-abuse/

Which Parental control guidance: http://www.which.co.uk/baby-and-child/child-safety-at-home/guides/parental-control-software/

How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-files-or-folders-on-your-.html

Get safe on line – Beginners Guide - http://www.getsafeonline.org/nqcontent.cfm?a_name=beginners_1

Childnet Parents and Teachers on downloading / music, film, TV and the internet - http://www.childnet.com/downloading/

Microsoft Family safety software: http://windows.microsoft.com/en-US/windows-vista/Protecting-your-kids-with-Family-Safety

Norton Online Family: https://onlinefamily.norton.com/

Forensic Software http://www.forensicsoftware.co.uk/education/clients.aspx

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

SSCB would like to acknowledge SWGfL for the use of their documentation.