Online Safety Policy

Adopted from the Local Authority	
Last reviewed on:	03/2023
Next review due by:	03/2025

RECORD OF AMENDMENTS

When Was the Plan last Updated?		
Date	**Name**	**Detail (changes made)**
Mar 2023	Cathy Varley	New Policy

Contents

Policy Introduction

The Online safety policy is in place to ensure that all staff and students are supported to understand how to keep themselves safe when using the internet and associated technologies. The use of these exciting and innovative technologies in school and at home has been shown to raise educational standards and promote student achievement. However, their use can put users at risk. These risks can be categorised into three main areas:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Bents Green School is committed to ensuring that students have safe access to the internet by putting effective systems in place to stop them accessing inappropriate information. This is reinforced by a curriculum which aims to ensure all students and staff develop a safe and responsible set of behaviours which will enable them to reduce the risks of harm whilst continuing to benefit from using the Internet and new technologies.

	Designated Safeguarding Lead (DSL)	Cathy Varley
	Online-safety lead	Cathy Varley
	Online-safety / safeguarding link governor	Natalie Brownell
	Online Safety Curriculum Coordinator (None Safeguarding)	Richard Cusworth Marie Old
	Network Manager / other technical support	George Sharp Lee McLean

	Date this policy was reviewed and by whom	Feb 2023 Cathy Varley
	Date of next review and by whom	Feb 2024 Cathy Varley

Aims

This policy aims to:

- Set out expectations for all Bents Green community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Scope of the Policy

- This policy applies to all members of the Bents Green School community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

- The **Education and Inspections Act 2006** empowers Head Teachers, 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 applies to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- The **Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Head Teacher believes it contains any illegal content or material that could be used to bully or harass others

- The school will identify within this policy how incidents will be managed and will, where appropriate, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Communication of the Policy

- The school's senior leadership team will be responsible for ensuring all members of school staff and students are aware of the existence and contents of the school online safety policy and the use of any new technology within school.
- The policy will be provided to and discussed with all members of staff formally.
- An online safety training programme will be established across the school to include a regular review of the online safety policy.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- The students Acceptable User policy will be developed in conjunction with the School Council to ensure the language and vocabulary is appropriate and understandable for the intended audience.
- Online safety modules will be included in the Knowledge for life and computing curriculum covering and detailing content of and amendments to the online safety policy / acceptable user policies.
- Pertinent points from the school online safety policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the online safety policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed online safety messages across the curriculum whenever the internet or related technologies are used
- The relevant sections of the online safety policy (Acceptable User policy) will be introduced to the students at the start of each school year
- Safeguarding posters will be prominently displayed around the school

Development / Monitoring / Review of this Policy

This policy has been developed through consultation with:

- Senior Leadership Team
- Safeguarding Team
    - Sheffield safeguarding partnership
- ICT Technical staff
- Governors

As a school Bents Green will keep abreast of new technologies and consider both the benefits for teaching and learning and also the risks from an online safety point of view. The online safety policy and procedures will be reviewed and amended as necessary.

The school will monitor the impact of the policy using:

- Logs of reported incidents via CPOMs and Smoothwall
- Internal monitoring data for network activity
- Surveys / questionnaires of students
    - parents / carers
    - staff

All staff and members of the School community will be informed of any relevant amendments to the policy.

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher – Key responsibilities

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Sheffield Safeguarding Children Partnership.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

Online safety lead - Key responsibilities

"*The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"*

- Ensure "An effective approach to online safety that empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."

- “Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.”
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and “undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework ‘Education for a Connected World – 2020 edition’) and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors and ensure staff are also aware
- Be aware and make judicious use of safeguarding reports that are produced by the schools Internet Monitoring Service by working in conjunction with technical teams.
- Make key decisions on allowing access to sites and apps in schools by relaxing either temporarily or permanently some of the filtering setting within the schools filtering and monitoring system and ensure that these decisions are logged. The DSL should prioritise keeping children safe but “be careful that ‘over blocking’ does not lead to unreasonable restrictions” (KCSIE 2021)
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex B
  - cascade knowledge of risks and opportunities throughout the organisation

Governing Body led by the Online Safety/Safeguarding Link Governor - Key responsibilities

(quotes are taken from Keeping Children Safe in Education 2021)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- "Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety curriuculum coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology."

Designated Safeguarding Lead/Deputies – key responsibilities

- To support the online safety coordinator in promoting an awareness and commitment to online safety throughout the school.
- To be a point of contact in school on online safety matters (see attached protocols) – receive and regularly review online safety incident logs and be aware of the procedures to be followed should an online safety incident happen in school.
- To lead the safeguarding team
- To liaise with the local authority, the Sheffield Safeguarding Children's Board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff, the Safeguarding governor, Senior Leadership Team, PSHCE and computing leads.
- To maintain an up to date understanding of current online safety issues, guidance and appropriate legislation.
- To ensure that online safety is promoted to parents and carers.
- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.

- To be aware of and understand cyberbullying and the use of social media for this purpose.
- To lead any investigations of illegal / inappropriate use of technology by students in line with behaviour and discipline procedures, reporting to and consulting with wider professionals in line with the schools responses to an Incident of Concern (see page 19)
- To attend Safeguarding Refresher yearly with Sheffield City Council.

All Staff – Key Responsibilities

- Recognise that **RSE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who Online Safety Lead (OSL) is- Cathy Varley DSL.
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting students remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide students when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment
- Read UKCIS Sharing Nudes and Semi –Nudes: How to Respond to an Incident.

- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- When supporting students remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.

Online Safety Curriculum Coordinator, PSHE lead and computing lead - Key Responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their students' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that students face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should now be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and students alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

- Ensure subject specific action plans also have an online-safety element
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.
- To work with the Senior Leadership Team and the school’s online safety coordinator to develop, implement and monitor a school wide online safety curriculum and protocols in line with current requirements and advice from the Safeguarding Sheffield Children’s board and other relevant establishments.
- To support the online safety coordinator and Senior Leadership Team to monitor the implementation of the online safety Acceptable Use Policies for students within school
- To work with the Senior Leadership Team and online safety coordinator to monitor the teaching and learning of online safety across school.
- To maintain up to date knowledge of current online safety issues and support the online safety coordinator to ensure that teaching staff receive guidance on what to teach / how to keep children safe online.
- Work with the online safety coordinator to provide schemes of work and reference to useful websites / activities / resources to support the teaching and learning relating to online safety
- Ensure that visual online safety information is clearly in place around school and that students are taught how to report a concern or problem.
- The computing lead to work with the SLT, the online safety coordinator and technical staff to develop safe and effective ICT systems and protocols across school.

Technical Lead - Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Support the HT and DSL team tom promote safe **remote-learning** procedures, rules and safeguards .
- Keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team and ensure safeguarding reports are manageable and appropriately shared,
- Maintain up-to-date documentation of the school’s online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school’s systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements
- To work with SLT and the computing lead to ensure appropriate filtering is in place for all students and that this is monitored and reviewed regularly and adapted as needed in line with new developments and the safeguarding log.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system, specifically
  - All externally facing devices shall be hardened and patched to ensure no high-risk vulnerable are present
  - All desktops shall have up to date anti-malware software installed
  - All incoming email shall be scanned for malware and filtered for spam
  - All anti-malware software shall be configured to alert the ICT technicians when any malware is detected
  - All malware definitions should be updated daily
  - All students access to the internet should be filtered for inappropriate use
  - All hard discs and other media containing school information (including backup media) should be securely deleted, either by specialist detection utilities or physical destruction prior to disposal
  - Data backups should be automated, taken at regular intervals (daily) and backup media should be kept offsite
  - Use a log consolidation tool in conjunction with a network time protocol server to enable accurate analysis of logs
  - All internet-facing systems shall be placed onto a separate network segment, a demilitarised zone (DMZ) with access to applicable services, controlled by a firewall
  - All wireless implementations shall be a minimum of WPA2 encryption, and shall require authentication prior to connection
- To support the school in providing a safe technical infrastructure to support teaching and learning
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.

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

  To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.

  To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.
- Where any external network traffic is allowed from the internet to the school, a local firewall will be deployed to restrict traffic into only necessary ports and IP.

Students - Key responsibilities

(To the best of their abilities)

- Read, understand and adhere to the student acceptable use policy and review this annually
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
- Help and support the school in the creation of online safety policies and practices and to adhere to any policies and practices the school creates.
- Know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- Know and understand school policies regarding cyberbullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Demonstrate awareness (where appropriate) of research skills and of legal issues relating to electronic content such as copyright laws.
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- Accept responsibility for comments made on social networking sites and/or text messages sent.
- Ensure you respect the feelings, rights and values of others in your use of technology in school and at home.

Parents/carers - Key responsibilities

- To help and support your school in promoting online safety
- Read, sign and promote the school's parental Acceptable Use Policy (AUP) and read the student AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, students or other parents/carers.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

- To take responsibility for learning about the benefits and risks of using the internet and other technologies that your children use in school and at home.
- To participate in online safety training events, either by attending workshops or by undertaking the online training provided on line.
- to support school in identifying parental training needs by completing online safety training audits when requested.
- To consult with the school if you have any concerns about your children's use of technology.
- Ensure that you monitor your child's use of the internet at home.

Data Protection Officer - Key responsibilities

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."
- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL schools for three market-leading GDPR compliance solutions at gdpr.lgfl.net
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Ensure that photographs are stored appropriately, shared in line with consent and kept for appropriate timescales.

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

Please also see "Guidance for Safer Working Practice for Adults who work with Children and Young People"

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 e.g. 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.
- Pass on to the safeguarding lead in school any occasions where students attempt to make contact with them personally (i.e. through a social networking site)
- 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.

Education and Curriculum

At Bents Green School we believe that the key to developing safe and responsible behaviours online, not only for students but for everyone within the school community, lies in a progressive and age appropriate online safety curriculum. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities that the Internet brings.

Online safety education will be provided in the following ways:

- We will provide a series of specific online safety-related lessons in every year group as part of the PSD AND PSHE, computing curriculum and other lessons as appropriate.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- We will remind students about their responsibilities through an Acceptable Use Policy which every student will sign and which will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- When searching the internet for information, students will be guided to use age-appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.

- Where appropriate students will be taught in an age / ability appropriate way about copyright in relation to online resources.
- Students will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be made aware of where / how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

Use of digital images, video and sound

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.

Bents Green School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff will inform and educate students about the risks associated with the taking, use of, sharing, publication and distribution of images. Students will be taught to understand the risks attached to inappropriate use of images / videos online. Staff will support students to develop safe and responsible online behaviours.
- Staff and students will follow the school policies on creating, using and storing digital resources – in particular:
    - Digital images, videos and sound will not be taken without the permission of participants (where possible)
    - Images and videos will be of appropriate activities and participants will be in appropriate dress
    - Full names of participants will not be used either with the resource itself, within the file name or in accompanying text online
    - Digital images and videos will not be published online without the permission of the staff / students involved.
    - Digital images will be uploaded to the media drive on the school's network or the 'Assessment for Learning App' as soon as possible and deleted from the device.
- Digital images, video and sound should only be taken on school equipment.
- Student's work can only be published with the permission of the student and parents or carers.

Managing ICT systems and access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.

- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- All laptops, computers, tablets and mobile phones accessing school networks will be locked down when not in use by the user, including the users own equipment if used to access school networks / email systems, whether the user is at home or in school.
- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All students will have an individual user account with an appropriate password which will be kept secure, in line with the student Acceptable Use Policy. They will (with staff support as needed) ensure they log out after each session.
- All student internet access will be monitored by staff and any concerns will be reported following the school's policies and protocols.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow students to access the internet through their id and password. They will abide by the school Acceptable User Policies at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. Lead Technician and Computing Lead Teacher
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur. All incidents of inappropriate access will be reported, investigated and acted upon appropriately.
- The school will regularly audit ICT use to establish if the online safety policy is adequate and that it is appropriately implemented across school. The policies will be reviewed and amended to minimise risks.

Filtering internet access

- The school uses a filtered internet service. The filtering system is provided by Virgin Media and Smoothwall.
- The school's internet provision will include filtering appropriate to the age and maturity of students. The online safety coordinator, headteacher and computing leads will meet to discuss steps to manage / develop the levels of filtering for different groups of students within school.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the Acceptable User Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Designated safeguarding Lead who will ensure that that the headteacher, online safety coordinator and lead technician are also informed. In the DSL's absence incidents should be reported directly to the Headteacher. The school will report such incidents to appropriate agencies including the local authority, (safeguarding advisory and/ or LADO {Local Authority Designated Officer}) police, CEOP (the Child Exploitation and Online Protection Centre) or the IWF(Internet Watch Foundation)

- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked. A record will be kept of requests and any changes to filtering.
- Students will be taught to assess content safely as their internet usage skills develop.
- Students will use age-appropriate tools to research internet content.

Passwords

- A secure and robust username and password convention exists for all system access. (Email, network access, school management information system).
- All students have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All staff have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All information systems require end users to change their password at first log on.
- All users are prompted to change their passwords at prearranged intervals.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and students have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and students will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, including:
  - Do not write down system passwords.
  - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
  - Always use your own personal passwords to access computer based services, never share these with other users.
  - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
  - Never save system-based usernames and passwords within an internet browser. ▪ All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the school's personal data policy.
- The school maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

- All users accessing school based information on personal devices must have those devices password protected. All devices should be set to request passwords if unused by the user after a 2 minute interval.

Management of assets

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

Data Protection

- We will ensure that all personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Users should ensure that they log off at the end of any session in which they are using personal data or that their computer is locked when left unattended.
- All sensitive information and personal data will be transferred using encryption and secure password protected devices. No personal information will be contained within the email body itself for any emails being sent to any external email accounts (not 'bentsgreen .sheffield.sch.uk' accounts)
- Personal or sensitive data will not be removed from the school site without permission of the headteacher and without ensuring that such data is kept secure.
- Personal data should never be stored on any portable computer system, USB stick or any other removable media.
- Staff should only save and use data using the onedrive system taking care to remove data once it is no longer needed.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Staff and students will not leave personal and sensitive printed documents on printers within public areas of the school.
- All physical information will be stored in controlled access areas.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.
- Staff accessing data using their own devices will ensure that they are not left unsupervised, that they are password protected and that settings are timed to require a password after 2 minutes of inactivity.

Using Email

- All students will use approved email accounts allocated to them by the school and be aware that their use of the school email system could be monitored and checked
- All staff should use approved email accounts for school business.
- Students will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening email from an unknown sender, or viewing / opening attachments.
- Communication between staff, students, parents / carers and members of the wider school community should be professional and related to school matters only
- Any inappropriate use of the schools email system, or the receipt of any inappropriate messages by a user should be reported using the schools reporting procedures.
- Any correspondence containing sensitive information / data will be sent through secure systems (encryption / secure password protected devices) via an attachment. No sensitive information will be contained within the email itself.
- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report to the headteacher 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, VLE etc.) must be professional in tone and content.

Using Fax machines

- All fax machines are situated within controlled areas of the school and any sensitive information or personal data sent fax is transferred using a secure method.

Using blogs, Wikis, podcasts and other ways for students to publish content online

- As we continue to develop and enhance our curriculum opportunities media such as blogs, wikis and podcasts (ways to publish content online) are used to enhance the curriculum by allowing students to publish their own content. However, we will always ensure that staff and students take part in these activities in a safe and responsible manner.
- Content will only be published within the school learning platform (or on recommended blog sites which require passwords, such as wordpress). Students will not be allowed to post or create content on sites where members of the public have access such that they can add content, make comments.
- Students will be reminded about safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, not to reveal personal information which may allow someone to identify and locate them. Students will not use their real names when creating such resources and will be supported to use appropriate nicknames.
- Parental permission will be obtained before any material is published online
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking and other online publishing outside of school.

Using mobile phones

- All students will be asked to hand in their mobile phones to reception on arrival at school.
- Students will collect their phones prior to going home.
- All students will be made aware that they cannot use their phones to take images of other students within school. Any incidents where students are found to have taken images of others on their phones will be reported immediately to the safeguarding team.

- Students may be allowed to use their mobile phones for specific learning activities such as offsite learning. Their use will be supervised by staff and students will be regularly reminded about the safe use of phones. Students will not be allowed to take photographs of other students.
- Staff will not provide their personal phone numbers to students. Where staff members are required to use a mobile phone for school duties they must take with them a school mobile phone.
- Staff should not use their personal mobile phones to make contact with students or parents / carers. If this is necessary, for example in an emergency situation, 141 should be placed in front of the number dialled to make the caller unidentifiable.
- If members of staff are personal friends or relatives of parents contact with parents on personal mobiles is acceptable out of school hours.
- Staff accessing email or the schools learning platform using personal mobile phones must ensure that they have appropriate security settings to protect personal data (as described under data protection and passwords).
- Staff should never use their mobile phones to take photographs of students.
- Mobile phones, as well as tablet and game systems, are a common vehicle for cyberbullying. All students will be reminded about the unacceptability of this during PSD AND PSHE lessons and otherwise as needed.

The school website and other online content published by the school

- The school website will not include the personal details, including individual email addresses, of staff or students.
- A generic contact email is used for all enquiries received through the school website
- All content for the school's website and twitter account will be published through the school's website team only and will be approved prior to publication.
- Permission will be gained from parents / carers to publish student photographs / information. Students' names will not be used alongside photographs.
- Staff and students should not post school-related content on any external website without seeking permission first from the Co-Headteachers.
- Governors photos on website

Communication Technologies

The grid below shows which technologies we have agreed as a staff will be allowed in school

	Students	**Staff**
Personal mobiles brought into school	Allowed but must be handed into reception/class and collected at the end of the day Allowed for some off-site activities with permission appropriate education / and supervision	Allowed in restricted areas of the school (offices, staffrooms and staff workrooms). They **should not** be used in classrooms or any other student areas. See mobile phone policy for exceptional circumstances

Taking photographs / videos on personal equipment	May be allowed on some offsite visits but not for taking photographs of other students. Must be closely monitored.	Not allowed
Taking photographs or videos on school's devices.	Allowed with permission	Allowed
Use of hand-held devices such as PDA's, MP3 players	Not allowed	Not allowed
Use of personal email addresses in school	Not allowed	Allowed at certain times
Use of online chat rooms in school	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Allowed at certain times
Use of blogs, wikis, podcasts	Allowed within learning activities under staff guidance and supervision	Allowed within guidance provided.
Use of video conferencing or other online meetings	Allowed within learning activities under staff guidance and supervision	Allowed for professional purposes

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:

- Deliberate access to illegal / inappropriate content
- Accidental access to illegal / inappropriate content
- Failure to report deliberate or accidental access to illegal / inappropriate content
- Inappropriate use of personal technologies within school, i.e. mobile phones
- Accessing non-educational websites during lesson time
- Sharing your username / password with others
- Failure to log off a computer when leaving the room
- Accessing school ICT systems using someone else's username / password
- Using school or personal equipment to send a message or create content that is offensive or bullying in nature.
- Attempting to circumnavigate school filtering, monitoring or other security settings
- Sending messages or create content which could bring the school into disrepute
- Revealing the personal information (including digital images, videos and text) of others without permission
- Use of online content in any way as to infringe copyright.
- Careless use of personal data, i.e. Insecure transfer of personal / sensitive data

- Use of digital communications to communicate inappropriately with students / parents (for example use of personal phones / emails to communicate, communication through social networking sites)
- Unauthorised downloading or uploading of files
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Actions which could compromise the staff member's or others' professional standing
- Any actions which could bring the school into disrepute or breach the integrity of the ethos of the school

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.

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

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct

The Safeguarding Sheffield Children's Board flow chart will be consulted and actions followed in line with the flow chart.

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. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures; by investigation led by the headteacher with guidance and support from human resources.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy

- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school or during extended periods away from school.

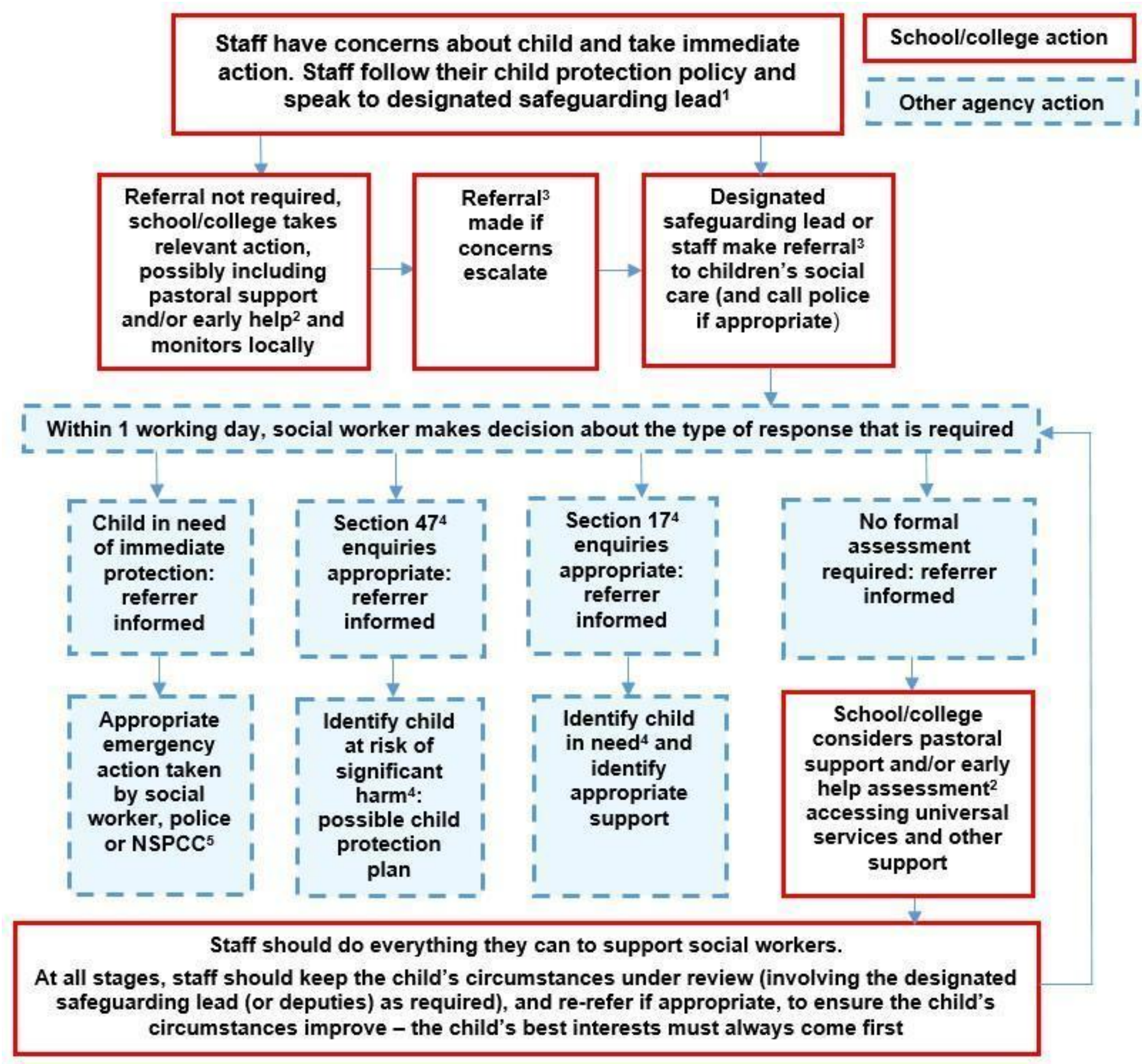
All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline

The school will actively seek support from other agencies as needed (i.e. the local authority, SCSP,
UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law

Actions where there are concerns about a child



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally

Referral[3] made if concerns escalate

Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47[4] enquiries appropriate: referrer informed

Section 17[4] enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC[5]

Identify child at risk of significant harm[4]: possible child protection plan

Identify child in need[4] and identify appropriate support

School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support

Staff should do everything they can to support social workers.

At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Further Information

Sheffield Schools and settings can consult with the online safety Project Manager on 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?online safety

“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/

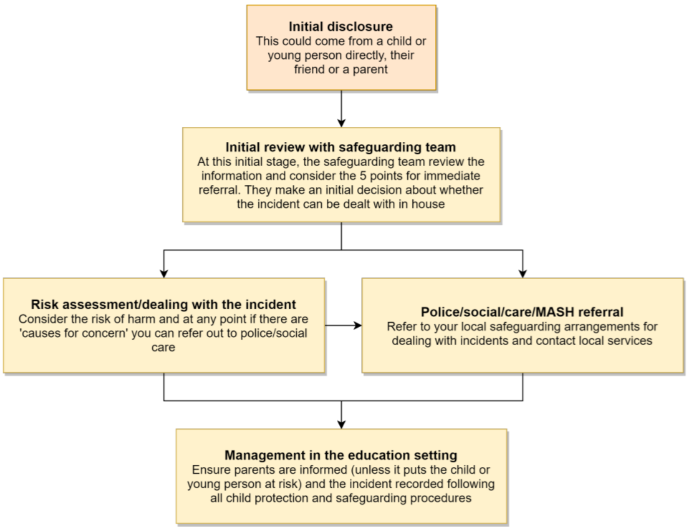
“Guidance for Safer Working Practice for Adults who Work with Children and Young People” (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.p

Sharing nude and semi-nude images

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any student in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right.

All staff are aware of this guidance:

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance.

Staff at Bents Green School foster a zero-tolerance culture of sexual harassment online and offline.

Bents Green School take all forms of sexual violence and harassment seriously, and recognise that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

Social media incidents

Bents Green School works on the principle that if we don’t manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first ‘googling’ the school, and the Ofsted pre-inspection check includes monitoring what is being said online

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools’ (and staff members’) online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Our Information Manager is responsible for managing our school Twitter Account. She follows the guidance in the LGfL / Safer Internet Centre online-reputation management document.

Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct/handbook (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals’ Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Staff, students’ and parents’ Social Media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the new Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

The school has an official Twitter account and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and students.

Students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the student or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.
The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 16) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Use of Mobile phones at Bents Green School, general issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets or in any classrooms or areas where students are present. Designated areas of the school where mobile phones can be used outside of teaching times include the staff room, staff work areas, staff offices and the school car park.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of the senior leadership team.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- All students are requested to hand in phones and personally-owned devices to reception/class on their way into school. For some activities, for example off-site life skills learning, students will be allowed to keep their mobile phones but will be reminded that they cannot use their phones to take images or videos and of the student Acceptable User policy.
- No images or videos should be taken on mobile phones or personally-owned mobile devices.
- Staff will be provided with school mobile phones to use for off-site activities.
- In exceptional circumstances staff may need to use their personal phones in an emergency situation. Where necessary for safety, personal phones can be used for staff to keep in touch with each other and to contact emergency services and school. Staff should avoid using personal phones to contact parents and families. If absolutely necessary (exceptional circumstances only such as a child absconding or seriously hurt) personal numbers will be protected by the use 141 prior to the family number being dialled.

Students’ use of personal devices

- If a student breaches the school Acceptable User policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- All students are requested to hand in phones and personally-owned devices to reception/class on their way into school. For some activities, for example off-site life skills learning, students will be allowed to keep their mobile phones but will be reminded that they cannot use their phones to take images or videos and of the other content within the student Acceptable User policy.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search student property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.
Full details of the school's search procedures are available in the school Behaviour Policy

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

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-andpractice/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-allby/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_y our_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/internetsafety_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-withtechnology-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-ofinternet-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-safetycontract.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_l earn.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-athome/guides/parental-control-software/

How to encrypt files: http://www.dummies.com/how-to/content/how-to-encrypt-important-files-orfolders-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/Protectingyour-kids-with-Family-Safety

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

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