

Kingsthorpe Grove Primary School



Online Safety Policy

Person(s) Responsible for Document: *Computing/ Online safety lead (Dan Bright)*

Relevant Committee: *Standards & Achievement Committee – 5th July 2021*

Date Document Ratified at Full Governing Body: 15th July 2021

Signed: 

Committee Chair

Signed: 

Chair of Governors


Signed: 

Head Teacher

Date Document to be reviewed: July 2022

Introduction:

Key People

| | | |
|---|--|---|
| <div>Kingsthorpe Grove Primary School</div>  | Designated Safeguarding Lead (DSL) team | Alison Dolan (Head teacher & Deputy DSL) Nicky Lovatt (Assistant Head/ Inclusion Manager & DSL) Yvonne Mooney (Family support & Deputy DSL) Lorraine Brown (Family support & Deputy DSL) |
| | Online-safety lead (if different) | Daniel Bright (Computing lead/ Class teacher) |
| | Online-safety / safeguarding link governor | Clive Rockell |
| | PSHE/RSHE lead | Kim Turney (Class teacher) |
| | Network manager / other technical support | Steve Cotter (Easi- PC) |

At Kingsthorpe Grove we aim to ensure that all of our policies take into account the rights of all children.

This policy aims to:

- Set out expectations for all Kingsthorpe Grove's 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, regardless of device or platform
- Facilitate the safe, responsible and respectful 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
 - 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)

The online safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new issues to online safety or incidents that have taken place.

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2020 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education and Computing. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy can be changed during the year in light of developments but is also subject to a full annual review. Acceptable Use Policies for different stakeholders help with keeping staff and pupils updated – these are reviewed alongside overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2020, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a risk that some pupils may have missed opportunities to disclose issues during the lockdowns.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply, students and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in corridors)

Contents

| | |
|---|-----------|
| <i>Introduction.....</i> | <i>1</i> |
| <i>Key People.....</i> | <i>1</i> |
| <i>Policy aims.....</i> | <i>1</i> |
| <i>What is this policy?.....</i> | <i>2</i> |
| <i>Who is it for; when is it reviewed?.....</i> | <i>2</i> |
| <i>What are the main online safety risks today?</i> | <i>2</i> |
| <i>How will this policy be communicated?.....</i> | <i>2</i> |
| <i>Scope of Policy.....</i> | <i>4</i> |
| <i>Schedule for Development, Monitoring and Review.....</i> | <i>4</i> |
| <i>Roles and Responsibilities.....</i> | <i>4</i> |
| <i>Education and information for parents and carers.....</i> | <i>12</i> |
| <i>Training of Staff and Governors.....</i> | <i>12</i> |
| <i>Technical Infrastructure.....</i> | <i>12</i> |
| <i>Assessment of risk.....</i> | <i>14</i> |
| <i>Reporting and Response to incidents.....</i> | <i>15</i> |
| Sexting | 16 |
| Upskirting | 16 |
| Bullying (Cyberbullying)..... | 16 |
| Sexual violence and harassment..... | 16 |
| Misuse of school technology (devices, systems, networks or platforms)..... | 16 |
| Social media incidents..... | 17 |
| <i>Data protection and data security.....</i> | <i>17</i> |
| <i>Appropriate filtering and monitoring</i> | <i>18</i> |
| <i>Electronic communications.....</i> | <i>18</i> |
| Email..... | 18 |
| School website..... | 19 |
| Cloud platforms..... | 19 |
| Digital images and video..... | 20 |
| Social media..... | 21 |
| Staff, pupils' and parents' Social media presence | 21 |
| <i>Device usage</i> | <i>22</i> |
| Personal devices including wearable technology and bring your own device (BYOD) | 22 |
| Network / internet access on school devices | 23 |
| Trips / events away from school | 23 |
| <i>Sanctions and Disciplinary proceedings.....</i> | <i>24</i> |
| <i>Sanctions: Pupils.....</i> | <i>25</i> |
| <i>Sanctions: Staff.....</i> | <i>26</i> |

Scope of Policy

This policy applies to all members of the KGPS community (including teaching and support staff, supply teachers, governors, volunteers, contractors, students/pupils, 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The implementation of the online safety policy will be monitored by the headteacher and reported to the Governors via the termly Headteacher's Report to Governors.

The impact of the policy will be monitored by the Computing lead by looking at:

- the log of reported incidents on MyConcern
- the Internet monitoring log (discussed weekly with Headteacher)
- surveys or questionnaires of learners, staff, parents and carers
- other documents and resources
- future developments

Roles and responsibilities

All members of the school community 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, pupils, 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.

Serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying will be recorded on MyConcern (in which DSL's and Online safety lead can access). If there is no access to MyConcern they are then to be recorded on an orange form, which is signed by the Head Teacher who reports it to the Governors and puts the original onto MyConcern.

| Role | Responsibility |
|--|---|
| Governors | <ul style="list-style-type: none"> • Approve and review the effectiveness of the online safety Policy • Delegate a governor to act as online safety link • Online safety Governor works with the online safety Leader to carry out regular monitoring and report to Governors |
| Head Teacher (Alison Dolan) Senior Leaders (Louise Brawn, Nicky Lovatt, Angela Woods) | <ul style="list-style-type: none"> • Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards • 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 • 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 DSL's 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 computing 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 the needs of pupils, 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 |

| | |
|--|--|
| <p>DSL's</p> <p>(Alison Dolan, Nicky Lovatt, Lorraine Brown, Yvonne Mooney)</p> <p>Online safety Leader</p> <p>(Daniel Bright)</p> | <ul style="list-style-type: none"> • Work with the HT and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards • Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised • Ensure an effective approach to online safety that empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate. • Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, and Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) • 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 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 • 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 • Receive regular updates in online safety issues and legislation, be aware of local and school trends • Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance 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 • Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues, 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. • Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown. • Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware |
|--|--|

| | |
|--|---|
| | <ul style="list-style-type: none"> • Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying • Facilitate training and advice for all staff, including supply teachers: <ul style="list-style-type: none"> ○ all staff must read KCSIE Part 1 and all those working with children Annex A ○ it would also be advisable for all staff to be aware of Annex C (online safety) |
| Other staff (Teachers, TA's, etc.) | <ul style="list-style-type: none"> • Recognise that RSHE 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 the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are • Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections). • 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 RSHE 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 pupils) • 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 • When supporting pupils remotely, be mindful of additional safeguarding considerations • Carefully supervise and guide pupils 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, plagiarism and GDPR. • Be aware of security best-practice at all times, including password protection and |

| | |
|---|--|
| | <p>phishing strategies.</p> <ul style="list-style-type: none"> • Prepare and check all online source and resources before using • Encourage pupils/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 low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this) • Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying, 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. |
| <p>PSHE/ RSHE lead</p> <p>(Kim Turney)</p> | <ul style="list-style-type: none"> • As listed in the 'other 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 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 pupils 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 lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach |

| | |
|---------------------------|---|
| Pupils | <ul style="list-style-type: none"> • Read, understand, sign and adhere to the pupil acceptable use policy and review this annually • Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen • 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 |
| Parents and Carers | <ul style="list-style-type: none"> • Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil 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 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, pupils or other parents/carers. • Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns • Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible. • 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. |

| | |
|--|---|
| <p>Technical Support Provider</p> <p>(Steve Cotter – Easi PC)</p> | <ul style="list-style-type: none"> • As listed in the 'other staff' section, plus: • Support the HT and DSL team as they review protections for pupils in the home and remote-learning procedures, rules and safeguards • Keep up to date with the school's online safety policy and technical information in order to effectively inform and update others as relevant • Work closely with the online safety lead 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 • 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 • Work with the Headteacher to ensure the school website meets statutory DfE requirements. |
| <p>Community Users</p> | <ul style="list-style-type: none"> • Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school • Support the school in promoting online safety and data protection • 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, pupils or other parents/carers • Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP • Maintain an awareness of current online safety issues and guidance • Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications |

Education of pupils

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, 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 pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

A progressive planned online safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Within this:

- key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches
- pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- pupils are taught about current issues such as online gaming, extremism, vlogging, use of social media and obsessive use of technology
- pupils will write and sign an Acceptable Use Policy for their class at the beginning of each school year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear Acceptable Use Policy guidance which they are asked to sign with their children and regular newsletter, website and class dojo updates.
- inviting parents to attend activities such as online safety assemblies or other meetings as appropriate;
- Providing guidance for parents and carers to help keep them informed and up-to-date on what they can do to help keep their child safe whilst online;
- providing and maintaining links to up to date information on the school website, class dojo and via the school Twitter account

Training of Staff and Governors

There is a planned programme of online safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the Acceptable Use Policies. This includes:

- **all** new staff and governors receiving online safety training as part of their induction programme
- providing information to supply and student teachers on the school's online safety procedures
- this online safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings

Technical Infrastructure

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's Acceptable Use Policy, in addition to the staff Acceptable Use Policy.

The school ensures, when working with our technical support provider, currently EasiPC, that the following guidelines are adhered to:

- the School IT systems are managed in ways that ensure that the school meets e-safety technical requirements
- there are regular reviews and audits of the safety and security of school IT systems.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
 - the downloading of executable files by users
 - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school

- the installing programs on school devices unless permission is given by the technical support provider or Computing subject leader
- the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)
- the installation of up to date virus software
- access to the school network and Internet will be controlled with regard to:
 - users having clearly defined access rights to school IT systems through group policies
 - staff users being made aware that they are responsible for the security of their username and password; they must not allow other users to access the systems using their log on details
 - the 'master/administrator' passwords are available to the Headteacher and the IT technician
 - users must immediately report any suspicion or evidence that there has been a breach of security
 - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff Acceptable Use Policy and are made aware of this e-safety policy
 - Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
 - Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
 - SEN Unit children will access either of the two bullet points above, depending upon their ability and understanding, which is to be agreed between the class teacher and the SEN Unit manager
- the Internet feed will be controlled with regard to:
 - the school maintaining a managed filtering service provided by an educational provider, currently Exa
 - the school monitoring Internet use
 - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team
 - filtering issues being reported immediately
- the IT System of the school will be monitored with regard to:
 - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems

- Online safety incidents being documented and reported immediately to the online safety Leader who will arrange for these to be dealt with immediately in accordance with the Acceptable Use Policy.

The following table shows how the school considers the way these methods of communication should be used.

| | Staff & other adults | | | | Pupils | | | |
|---|----------------------|----------------------------------|--------------------------|-------------|---------|--------------------------|-------------------------------|-------------|
| | Allowed | Allowed at certain times/ places | Allowed for select staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Communication Technologies | | | | | | | | |
| Mobile phones may be brought to school | ✓ | | | | | | ✓ | |
| Use of mobile phones in lessons | | | | ✓ | | | | ✓ |
| Use of mobile phones in social time | | ✓ | | | | | | ✓ |
| Taking photos on mobile phones or other camera devices | | | | ✓ | | | | ✓ |
| Use of personal devices | | | ✓ | | | | | ✓ |
| Use of personal email addresses in school, or on school network | | | | ✓ | | | | ✓ |
| Use of school email for personal emails | | | | ✓ | | | | ✓ |
| Use of chat rooms / facilities | | | | ✓ | | | | ✓ |
| Use of messaging apps | | | | ✓ | | | | ✓ |
| Use of social networking sites | | | | ✓ | | | | ✓ |
| Use of blogs | ✓ | | | | | ✓ | | |
| Use of Twitter | | | ✓ | | | | | ✓ |
| Use of video broadcasting e.g. Youtube | | | | ✓ | | | | ✓ |

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the online safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Northamptonshire County Council can accept liability for the material accessed, or any consequences resulting from Internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to 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).

General concerns must be handled in the same way as any other safeguarding concern; 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, 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 (including school sanctions)
- Acceptable Use Policies
- Prevent 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 on pupils 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 them to be dealt with 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 respond to illegal and inappropriate incidents through a thorough investigation. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of Child abuse then the monitoring will be halted and referred to the Police immediately.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

If an incident or concern needs to be passed beyond the school then the concern will be escalated to the Local Authority Designated Officer (LADO)
01604 362993

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools.

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 Sexting; 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, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

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

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 pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying (Cyberbullying)

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.

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.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device).

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Kingsthorpe Grove Primary School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) 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, Kingsthorpe Grove Primary 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 (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

There are 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), which the DSL's will seek to apply.

"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."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The Headteacher and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of password encryption for non-internal emails is compulsory for sharing pupil data. If this is not possible, the DSL should be informed in advance. GDPR rules apply to the following:

- CCTV
- Use of personal vs school devices
- Password policy / two-factor authentication
- Device encryption
- Access to and access audit logs for school systems

- Backups
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies
- BYOD
- Wireless access
- File sharing
- Cloud platform use, access and sharing protocols

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

We have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called Surfprotect.

There are three types of appropriate monitoring identified by the Safer Internet Centre.

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At home during periods of isolation, school devices are monitored on return for any safeguarding concerns in regards to Prevent. (Pupils and parents sign an agreement on Acceptable use of these devices before they are issued)

When pupils log into any school system on a personal device, activity may also be monitored using Gsuite admin console.

Electronic communications

This section covers electronic communications, but appropriate conduct and audit trail apply.

Email

- Pupils at this school use the Gmail, Gsuite for school emails (this is currently disabled)
- Staff at this school use the exa system for all school emails

Both these systems are auditable, trackable and managed. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email (including Google classroom comments, class dojo messages) is a means of electronic communication used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the Headteacher in advance. Any unauthorised attempt to use a different system 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).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
 - If data needs to be shared with external agencies permission should be sought by DSL's
 - Internally, staff should use the school network, including when working from home when remote access is available
- Pupils are restricted to emailing within the school and cannot email external accounts
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value.

The DfE has determined information which must be available on a school website.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service (Google drive, Google classroom, Gsuite, class dojo).

The following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud
- The Headteacher approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such

- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At KGPS, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos). This is always given permission by a DSL.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

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

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

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

KGPS 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 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.

Lindsey Coe (PA to Headteacher) is responsible for managing our Twitter account. Angela Woods (SENCO) is responsible for managing our school Youtube account. Daniel Bright (Computing. Online Safety lead) is responsible for managing Class dojo and Google classroom accounts.

Staff, pupils' 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 pupils 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 in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils 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 pupils/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 pupils/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).

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

Email (including class dojo and google classroom) is the official electronic communication channel between parents and the school, and between staff and pupils.

Pupils/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.

Pupils/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 and should be declared upon entry of the pupil 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 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.

Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils in Years 5/6** are allowed to bring mobile phones in for emergency use/communication with parents and carers if they walk to school. Within school, phones must remain turned off at all times and given to the class teacher to lock away. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to consequences listed in the Behaviour policy and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may have their phone on their person but must arrange staff to cover when leaving to take the call in a private staff area away from children.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take

photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.

- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events the Headteacher will inform parents of consent for photos/videos. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **Pupils** are not allowed the school Wi-Fi access via personal devices.
- **Home devices** are issued to some students. These may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number. (141)

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 pupils/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

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users 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
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet

In addition, the following indicates school policy on these uses of the Internet:

| | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable |
|-----------------------------------|------------|-----------------------------|--------------------------------|--------------|
| Online gaming (educational) | | ✓ | | |
| Online gaming (non-educational) | | | | ✓ |
| Online gambling | | | | ✓ |
| Online shopping / commerce | | | | ✓ |
| File sharing (using p2p networks) | | | | ✓ |

Sanctions: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Behaviour Policy.

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, ticks may appear in more than one column.

The ticks in place are actions which must be followed.

| Incidents | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | 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). | | ✓ | | ✓ | | | |
| Unauthorised use of non-educational sites during lessons | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Unauthorised use of mobile phone / digital camera / other handheld device | ✓ | | | ✓ | | | ✓ |
| Unauthorised use of social networking / instant messaging / personal email | ✓ | | | ✓ | ✓ | | ✓ |
| Unauthorised downloading or uploading of files | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| Allowing others to access school network by sharing username and passwords | ✓ | | | | | ✓ | |
| Attempting to access or accessing the school network, using another pupil's account | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Attempting to access or accessing the school network, using the account of a member of staff | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Corrupting or destroying the data of other users | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Continued infringements of the above, following previous warnings or sanctions | ✓ | | | ✓ | ✓ | | ✓ |
| Actions which could bring the school 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 | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Accidentally accessing offensive or pornographic material and failing to report the incident | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Deliberately accessing or trying to access offensive or pornographic material | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | ✓ | | ✓ | ✓ | ✓ | | ✓ |

Sanctions: Staff

Schools should populate the grid below marking appropriate possible sanctions.

Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore, marks may appear in more than one column.

The marks in place are actions which must be followed.

| Incidents: | Refer to Head teacher | Refer to Local Authority / HR | Refer to LADO(L)/Police(P) | 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). | ✓ | ✓ | L,P | ✓ | | ✓ | ✓ |
| Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email | ✓ | | | ✓ | ✓ | | ✓ |
| Unauthorised downloading or uploading of files | ✓ | | | ✓ | ✓ | | ? |
| 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 | ✓ | | | ✓ | ✓ | | ✓ |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| 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 | ✓ | | | ✓ | ✓ | ✓ | ✓ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature staff | ✓ | ✓ | L,P | ✓ | | ✓ | ✓ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners | ✓ | ✓ | L,P | ✓ | | ✓ | ✓ |
| Breach of the school Online safety policies in relation to communication with learners | ✓ | ✓ | L | ✓ | | ✓ | ✓ |
| Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils? | ✓ | ✓ | L | ✓ | | ✓ | ✓ |
| Actions which could compromise the staff member's professional standing | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Actions which could bring the school 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 | ✓ | ✓ | | ✓ | | | ✓ |
| Accidentally accessing offensive or pornographic material and failing to report the incident | ✓ | ✓ | L | ✓ | ✓ | ✓ | ✓ |
| Deliberately accessing or trying to access offensive or pornographic material | ✓ | ✓ | L,P | ✓ | | | ✓ |
| Breaching copyright or licensing regulations | ✓ | ✓ | | ✓ | | ✓ | ✓ |
| Continued infringements of the above, following previous warnings or sanctions | | | | | | | |