Policy Statement

Subject	eSafeguarding
Coordinator	P. Jones
Date	May 2017
Review Date	2020/2021

eSafeguarding

This policy statement contains information on the safeguarding aspects of Information Technology.

It covers a range of devices which include but are not limited to:

- Computers and laptops
- iPads and tablets
- iPods
- Kindles and generic eReaders
- Smartphones and watches
- Games consoles (Playstations, X-Boxes etc)
- Video or streaming devices

It includes all aspects of internet use and online safety.

Background

Information technologies give us powerful tools, which open up opportunities for everyone. They are essential to modern study and the worlds of work, leisure and commerce. However, they also bring dangers.

Schools have a duty under the national curriculum not only to teach pupils how to use these technologies effectively and creatively, but also how to stay safe.

Linked policies

- Safeguarding
- Anti-bullying
- Prevent
- Staff Code of Conduct
- Staff Discipline, Conduct and Grievance
- ICT
- PHSCE
- Data Protection

Risks

Risks include:

- Exposure or access to text or images that are illegal or simply inappropriate
- Excessive use to the detriment of other aspects of personal and educational development
- Being groomed or abused
- Involvement in the sharing of Youth Produced Sexual Images ('Sexting')
- Cyber-bullying
- Illegal downloading/copyright infringement
- Loss or inadvertent sharing of personal information, including through Location Services
- Reckless sharing of personal information with strangers
- Scams, fraud, and phishing
- Use of games or apps containing unsuitable material (outside Age Range guidance)
- Inability to question what is fact and what is opinion, and to use online materials uncritically
- Plagiarism (copying material and passing it off as your own work)
- Sharing personal images without appropriate consent
- Accessing information or sites to which you have no right ('hacking'), or being hacked
- Failure to understand that the internet is not in itself a safe and private place, but that individuals can take precautions to make it safer and control their privacy settings to a degree

Not all risks can be completely eliminated, but children must be taught to understand and minimise them.

For adults to be able to do this and to protect and guide children, they must be aware of the constantly changing risks as digital devices and technologies keep evolving.

Policy consultation and review

eSafety is a standing agenda item for the school IT Group which meets weekly. The core group comprises the Lead Teacher for IT, technician and network manager. It is also a standing agenda item for the School Council, enabling pupil perspectives and opinions to inform policy and practice. Representatives can take concerns and ideas from their classes following discussion.

The school eSafeguarding Group comprises the Designated Safeguarding Lead; the eSafety Lead (if different); the Headteacher; the Safeguarding Governor; the Curriculum Lead for IT; the IT Meeting Manager. It forms the link between all parts of school, including pupils (the Schools Council) and the Governing Body. It ensures that policy and practice is kept under review and meets at least termly.

The Governing Body is involved through the nominated link Governor for Safeguarding (see website for details), who regularly meets the Safeguarding Lead and acts as a two-way channel of communication, as well as participating in the regular eSafeguarding Group meetings.

This policy, including all policy into practice guidance, is reviewed at least annually.

Monitoring

School monitors the impact of this policy through the review of records from several sources:

- Incidents recorded securely on the Child Protection Online Management System (CPOMS). Within this, there is an easily identifiable eSafety sub-category within the overarching category of Safeguarding.
- A hard-copy 'Securus' file containing details of all incidents identified and investigated through network monitoring systems. The eSafeguarding Lead is responsible for ensuring this occurs.
- A hard-copy 'Lightspeed' file containing details of all incidents identified and investigated through network filtering systems. The eSafeguarding Lead is responsible for ensuring this occurs.

- Pupil, staff and parent eSafeguarding data gathered through the Bradford Council Children's Services eSafeguarding questionnaire, reviewed annually and linked to eSafety week activities:

www.surveymonkey.com/s/pupilesafety

www.surveymonkey.com/s/adultesafety

www.surveymonkey.com/s/parentsesafety

Additionally, there is robust external review and audit of systems, eg through the 360DegreeSafe accreditation process.

Roles and responsibilities

The Governing Body is responsible for the approval of the eSafeguarding policy and reviewing its effectiveness.

It appoints a Governor for eSafety.

The Governor for eSafety meets the teacher responsible for the day-to-day eSafety arrangements, and attends the termly meeting of the eSafeguarding Group and reports back to Governors.

The Headteacher has responsibility for all aspects of safeguarding in school but delegates day to day arrangements to the eSafety Lead. The Headteacher must ensure that this person has sufficient training, time and resources to fulfil the role effectively. The Headteacher must also take appropriate action in the event of any eSafety infringement or breach of Acceptable Use Agreement by any member of the school community.

The Safeguarding Lead ensures that eSafety is led, managed and given due weight within the wider context of Safeguarding. S/he is best placed to evaluate eSafety concerns about individuals and families, which might sit within a broader range of concerns.

The eSafety Lead, who may also be the Safeguarding Lead, ensures that monitoring and filtering systems are working effectively and that incidents are reviewed as they occur. This happens within 24 hours during school workdays and on the first day back after a weekend or holiday. Files are kept for review. The eSafety Lead also co-ordinates eSafety training for pupils, staff and parents, including eSafety week and the induction of new staff. The eSafety Lead convenes and chairs the school eSafety Group and is responsible for keeping Governors updated about online safety issues, either directly or through liaison with the nominated Governor. If different, the eSafety Lead will also work closely with the Designated Safeguarding Lead and ensure that eSafety concerns are followed up and recorded on CPOMS. The eSafety Lead will follow the steps described in *Managing Incidents* in the practice guidance that supports this policy.

Staff must understand the importance of eSafety and how to ensure that they and pupils stay safe online. They must have read, understood and signed the Acceptable Use Agreement (AUA) and adhere to the Code of Conduct for adults working in school. The must teach pupils how to stay safe and ensure that they understand and adhere to their own AUA. They must report any breaches or risks to the eSafety Lead. They contribute to developing policy and practice through surveys, evaluations and professional vigilance.

The technical manager for IT must ensure that the school's infrastructure is secure and not open to malicious attack or misuse, and keep up-to-date with relevant technologies. This includes ensuring that monitoring and anti-viral software is upgraded as required.

The curriculum leader reviews curricular provision in school and ensures that eSafety is taught systematically and embedded in good practice across the curriculum.

Pupils must understand the appropriate AUA (which may be called 'rules' or a 'code of conduct') and keep within it at all times. They are involved in developing policy and practice through surveys, the School Council and discussions within the curriculum and eSafety week.

Parents/carers must sign an AUA before their children are allowed to access school equipment. They are responsible for supporting their children's learning by upholding high standards of eSafety at home. This includes respecting the eSafety of others in the school community. They are involved in developing policy and practice through surveys, the school app, and meetings during eSafety week.

Visitors who use school IT facilities must also sign the AUA and only use equipment that has been logged out to them under their own name. They must not connect to the school network via personal devices.

eSafety Curriculum

A strong eSafety curriculum helps to keep children safe in school, at home, and in their future lives.

We follow the Curriculum Innovation Computing Scheme of Work which has a robust and comprehensive eSafety strand. As they progress through school, children learn more and more about how to use technology as safely as possible, and what to do if things go wrong.

Mobile Devices

Staff and adults in school must only use mobile devices such as phones, smartphones and tablets in accordance with the strict school guidelines, AUA, safeguarding policy and code of conduct. The school's rules are detailed in the Policy into Practice documentation.

Parents sign to say they will not use devices to film or photograph or otherwise record other members of the school community without their consent (or in the case of children the consent of their parents).

Parents, visitors and contractors should not use devices in toilets, bathrooms or any areas where children change. Calls should be made and taken away from children and switched off or put on silent during meetings. No device brought onto the site may contain inappropriate or illegal content.

Pupils are not allowed to bring devices into school or onto the school site under any circumstances.

Personal mobiles should not be logged onto the school wi-fi.

Other Personal Equipment

The policy and AUAs are clear that children should not bring devices from home. Very occasionally, a child may want to share work done out of school which is stored on a device such as a USB or other portable drive. Exceptionally, a staff member may agree to this but if this happens, they become responsible for ensuring that the device is passed to the IT Technician for virus scanning before it is connected in any way to the school IT system, and for ensuring that content is suitable. Where others from outside school bring in digital materials (eg for staff training, multi-agency meetings or as part of a job interview) they must either use these on their own equipment without connecting to the school system, or else arrive in sufficient time to have virus screening performed by school IT staff.

Copyright and plagiarism

'Digital isn't Different,' and copyright applies just as much to using digital technologies and the internet as it does to using books or television programmes in schools. However, the working speed of digital technologies is such that significant movements between different copyright situations become blurred and even invisible. Materials can be altered and re-shared very rapidly in in a multitude of formats. Fundamentally, schools, teachers and pupils meet copyright in four different roles as users or consumers; as re-users; as publishers or distributors and as authors or creators.

There is an increasing amount of material freely available through the internet which can be used without seeking permission or paying for a licence, but it is vital to know what materials can and cannot be freely used or shared.

In the UK, copyright is a 'property' and using it is based on permissions: sometimes you have to ask and abide by the response you get. There is no general exception to copyright for schools and to use anything because "it's for teaching and learning" without having the necessary permissions to do so is to risk prosecution.

Using digital materials for individual learning is not the same as sharing those materials with other people. There is a clear distinction between using something yourself and passing it on. Nothing should be stored on the school server, published on the web or shared through an online service without having any necessary permission.

The whole area is fraught with complexity and will be for the foreseeable future as technologies and media change. Copyright, like everything else, is developing its regulation and practice in the face of new digital technologies and models of use and business.

This section itself draws on Copy Rights and Wrongs (http://www.copyrightsandwrongs.nen.gov.uk)

Additionally, pupils have to learn they must acknowledge sources, give credit to others for their work and never to attempt to pass off someone else's work as their own.

Handling eSafety complaints, referrals and incidents

- Complaints of misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Safeguarding issues are dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure via the school brochure.
- In cases of illegal and potentially criminal activity, issues will be referred to the police.

More detailed guidance for staff is published in the Policy into Practice document that accompanies this policy.

The authority of the Headteacher in relation to incidents that occur outside school

By law, the Headteacher has the authority to investigate and act to control behaviour away from the school site. He or she

"…may, to such extent as is reasonable, include measures to be taken with a view to regulating the conduct of pupils at a time when they are not on the premises of the school and are not under the lawful control or charge of a member of the staff of the school"

(Section 89 (5) Education and Inspections Act 2006)

Searches and sanctions

Under the same law, the Headteacher has the authority to search a pupil. Any search is in accordance with strict regulations as set out by law and detailed in the Policy to Practice section and the Safeguarding policy.

Policy into Practice

Ways for children to raise concerns

Children may raise concerns about eSafety in a range of ways but should always begin by taking themselves away from the source of distress, whether this is by stopping engaging in a 'chat', closing a lid, or turning over an iPad.

- Tell a trusted adult (eg parent or teacher)
- Use an 'alert' button or icon
- Go to the Safeguarding Lead in school (posters displayed throughout school)

If there is no immediate risk, they can:

- Raise the matter through the pupil survey
- Report through their class councillor

Internet

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the internet and linked content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Bradford City Council can accept liability for the material accessed, or any consequences of internet access.

- Children are taught to immediately shut the lid of a laptop or turn over an iPad if they come across anything they think is wrong or makes them feel uncomfortable. They must then tell an adult straight away.

- If staff or pupils discover unsuitable sites or content, the URL (address), time, content must be reported to the monitoring helpdesk via the eSafeguarding Lead or network manager. All cases are followed up and discussed by the eSafety group to ensure that similar incidents do not happen again and any known gaps in the firewall are plugged.

- School ensures that the use of internet derived materials by pupils and staff complies with copyright law.

- Pupils are taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

- Staff using sites such as YouTube should always plan and watch material first. Even so, comments and advertising material cannot always be avoided if sites are used 'live', so teachers should only display content to pupils in full screen mode.

- Children are taught only to use Safe Search from school devices. If, when working with children, staff need to access text or images that are not available through Safe Search, they should prepare in advance and save and access them via Dropbox.

Passwords

Pupils are taught that they must always log in as themselves.

They are taught never to disclose their password to others or to write it down.

They are taught to understand the importance of strong passwords. However, the younger children in school struggle to remember complex passwords so our approach is to require pupils to use passwords that become increasingly sophisticated as they move through school.

The IT Manager maintains a physical list of passwords and it is important that this is kept secure, private and not copied beyond what is necessary to enable lessons to run smoothly. Thus, a class teacher may need a copy in order to assist a pupil who has forgotten their password, but it would not be appropriate to distribute several copies of the 'master list' around a classroom.

Key Stage 1: children use a simple word from the high frequency word list eg dog

Year 3 and 4: they add a digit each year, eg Y3 d0g or dog4; Y4 d0g1 or 1dog4
Year 5 and 6: children add characters until they have 6-10 characters in total, including at least one numeral, one lower case and one upper case letter, eg D0g1Fi3h
Allowances may need to be made for children with special educational needs.

In this way, the password grows in complexity as the children get older and they come to understand the importance of having confidential passwords that are extremely strong.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Refer to the school's Data Protection policy for further details.

Encryption of devices: to reduce the possibility of sensitive or confidential information becoming compromised if a device is lost or stolen, all computers including staff laptops are securely encrypted using Bitlocker.

iPads and iPods are automatically encrypted and guarded by a passcode.

Cyberbullying, sexting and other misuse of IT

Childnet International defines cyberbullying as a type of aggression relating to the "sending or posting of harmful or cruel text or images using the internet or other digital communication devices".

Cyberbullying is dealt with in the same way as other types of bullying. We operate a zero-tolerance code of practice. We always involve parents, explaining their responsibilities and showing them what their child has done.
Children are taught about cyberbullying and what to do if they experience it. This forms part of the eSafety strand in our scheme of work.

In terms of disciplinary measures a school can take, cyberbullying falls within the remit of the Education and Inspections Act 2006. This requires Headteachers to promote discipline, good behaviour and prevent all forms of bullying. Headteachers have the power to take measures to "such an extent as is reasonable". The act also allows for the confiscation of items, including mobile phones, from pupils who misuse them − whether inside, or outside school. This legislation also sends a strong message to parents and pupils that bullying will not be tolerated, with court-imposed parenting orders to compel parents of bullies to attend parenting classes or face fines of up to £1,000.

We also advise parents that we do not recommend that pupils of primary school age have their own social media accounts. To do so infringes the regulations and guidance of most of the platforms themselves and our experience tells us that children of this age find it very hard to 'get it right' socially when using social media apps, and struggle with the levels of social awareness, self-control, empathy and 'netiquette' necessary to use these media successfully. Naivety and inappropriateness can easily be interpreted as bullying by the person on the receiving end and potentially serious situations can arise very suddenly.

Not having accounts also largely eliminates the risk of *sexting.*

Sexting

Sexting itself involves the sharing of sexual images or text with or by a minor.

If sexting is reported, an initial meeting is required to consider the available facts and decide on a course of action. If possible, offending imagery should not be viewed.

An immediate referral to police and/or Children's Social Care must be made if:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

4. The imagery involves sexual acts and any pupil in the imagery is under 13.
5. There is reason to believe a young person is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply then the Safeguarding Lead may decide to respond to the incident without involving the police or children's social care. However, an incident may be escalated at any time if further information/concerns come to light).

Further detailed guidance is available by reference to *Sexting in Schools and Colleges* (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF)

Email

Pupils may only use approved email accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Whole class or group email addresses should be used in school.
- Access in school to external personal email accounts may be blocked.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Media

- We block access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location, and not to place personal photos on any social network site.
- Pupils are advised on security and encouraged to set strong passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Children are taught the importance of being polite and appropriate in their online interactions, asking themselves the question 'Would I be happy for my parent/teacher to see this?'
- Outside school, parents and pupils are advised to heed advice and regulations about minimum ages recommended for different social media apps and platforms.
- School uses text messaging and MySchool App to communicate with families.
- Older children may be taught to use social media responsibly. This will only be in a sheltered environment, benefiting from protective privacy settings and safeguards. They must not however use any social medium in school unless it has been approved by a teacher. The teacher is responsible for ensuring that the pupils understand where, when and how they can use it.
- Adults working in school must keep their professional and private lives separate. Where they are identifiable as part of the school community or engage in social media in a professional capacity (for example by saying they work in a school) they are expected to maintain the highest professional standards. They must establish appropriate and robust privacy settings and respect others' need for privacy too.

- A teacher in school might use (for example) Twitter or TES forum to research educational developments or to find ideas or best practice to inform planning. This is acceptable use of social media in school.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Cloud Storage and Dropbox

These may not afford sufficient security and it should not be assumed that pictures and other data stored in these locations are private. To reduce risks, Dropbox should be used as a medium by which to transfer files and not as a storage solution. If in doubt staff managing IT in the school should refer to the latest DFE guidance: Cloud (educational apps) software services and the Data Protection Act. This was last updated 7.3.17 at time of writing but by its nature is revised regularly as technologies develop rapidly.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or when with or around children.
- Staff will have use of a school phone where contact with pupils is required.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies. Staff use of mobiles is considered in more detail in the section immediately following the table.

	Staff			Pupils			
Communication Technologies	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Phones and personal devices may be brought to school	x						x
Phones and personal devices may be used in lesson time			x				x
Phones and other personal devices may be used at school in social time	x						x
Taking photos on any device other than school equipment			x				x
Use of personal email addresses in school, or on school network, or on school business			x				x
Use of school email for personal emails		x		x			
Use of chat rooms / facilities other than purposes of teaching			x		x		
Use of instant messaging		x					x
Use of social media in school for educational purposes		x			x		
Use of blogs		x			x		

Use of mobile devices by staff

Staff may have personal mobile devices on their person in school. However, their use is strictly limited.

They may be used only during official breaks, and not in the presence of children.

The only exceptions to this are:

1. In an emergency, when it the phone may be used to summon assistance from the office, school leaders, or emergency services through a 999 call;
2. On a trip or visit when it may be necessary to contact school, and a school mobile is unavailable or has no signal.

School equipment must always be used to record children or their work and never uploaded or otherwise transferred to personal devices or storage areas.

School phones must wherever possible be used on and for school business.

A personal mobile should never be used to contact parents or pupils.

During teaching time and at other times when working (for example, when on playground duty or attending a meeting) devices must be switched off or put into silent mode, except in exceptional circumstances agreed beforehand with a senior leader. This includes wearable technology. Staff may however check the time on a device if they do not have access to an accurate clock or watch.

Published Content and the School Website

- The contact details on the website are the school address, email and telephone number. Personal information relating to anyone in the school community should never be published.
- The Headteacher or his/her delegated representative takes editorial responsibility and ensures that content is accurate and appropriate.

Images

- Permission from parents or carers is obtained before photographs of pupils are published on the school website. Where photographs or videos are published, names will not. Pupils' full names will never be published.
- Parents must sign a photograph consent form in which they undertake not to put images of other children on social media or the internet without the express permission of the other children's parents.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. (See 'Internet' above.)
- The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.

Managing Incidents

Incident	**Speak to/inform**	**Action**
Theft or loss of sensitive data: I. Lost or stolen device, or II. Unauthorised access to website, network or staff email (hacking)	Headteacher Contact police if theft occurs off school premises	List any information which could have been compromised. List any password protected services and change all passwords immediately. Necessary contacts may include: • Information Commissioner, if a data-breach is 'serious': see https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf • Persons affected by loss of personal data • Insurers
Inappropriate contact online or otherwise through device: Child has been contacted inappropriately on social media, through gaming, email, text, or other means. This includes unsolicited calls and	Safeguarding Lead	Preserve evidence, eg by taking screen shot Follow safeguarding procedures, contacting parents, Child Protection and/or police as appropriate Consider reporting to CEOP Reinforce eSafety education for child and peers

contacts made on a mobile phone.		
Exposure in school to inappropriate materials: Child has been accidentally exposed to unsuitable content in image, text or media. This includes (but is not limited to) pornography, violence, bad language, racism and sexism.	Safeguarding Lead IT technical team	Isolate the device Preserve and review evidence Consider and act upon any breach of rules, Codes of Conduct or AUA In cases of possible illegality, refer to police Review filters and firewalls
Inappropriate or risky behaviour by pupils online or on the network at school, including use of rude language	Safeguarding Lead	Preserve and review evidence Check previous record of pupil: prior eSafety warnings on paper file or CPOMS; user logs on Securus Consider breach of AUA and sanction accordingly. Misuse of equipment can result in a ban Speak to pupil Decide whether to speak to parent Consider using opportunity to discuss eSafety with class/year group Log on CPOMS (eSafeguarding category)
Inappropriate or risky pupil behaviour online or using devices out of school	Safeguarding Lead	Check previous record of pupil: prior eSafety warnings on paper file or CPOMS Speak to pupil Speak to parent Contact Children's Social Care and /or police if appropriate Log on CPOMS (eSafeguarding category)
Bullying: Harassment, threats, defamation, insults, ridicule or abuse directed at any member of the school community online or through devices	Safeguarding Lead	Preserve and review evidence Check previous record: prior eSafety warnings on paper files or CPOMS; also, for pupils, prior behavioural warnings for related offences in Behaviour records Speak to victim and perpetrator If a child is involved, speak to parent Consider PHSCE work with pupil(s) Contact Children's Social Care if appropriate Consider referral to police and/or legal services Consider reporting in bullying data to the local authority

		Log on CPOMS (eSafeguarding category) or other record as appropriate Teachers who have been abused online can contact the UK Safer Internet Centre on 0844 381 4772; email helpline@saferinternet.org.uk and/or may seek help through a professional body such as a union
Digital lifestyle behaviours: Obsessive or uncontrolled use of devices to the detriment of a full, balanced and healthy lifestyle	Safeguarding Lead	Check previous record of pupil: prior eSafety warnings on paper file or CPOMS Speak to pupil Speak to parent Consider referral to School Nursing Service Contact Children's Social Care and /or police if appropriate Log on CPOMS (eSafeguarding category)
Breach of copyright: Downloading and using copyright protected material without permission. This includes image, text, audio and video.	Headteacher and Business Manager	Preserve and review evidence Decide if any action needs to be taken For staff, consider training, including knowledge of sources of copyright free, and creative commons images and sounds For pupils, consider teaching implications, ensuring that copyright and attribution issues are covered sufficiently

Searches and sanctions

Under (Section 89 (5) Education and Inspections Act 2006), the Headteacher can search a student or their possessions for **any** item with their consent. Formal written consent is not required. If member of staff suspects a student holds an item banned by school rules and a student refuses a search, school can apply a disciplinary penalty.

However, as mobile phones and devices are prohibited items under the school rules and this policy, consent for a search is not required as long as the member of staff has reasonable grounds to suspect that the student is in possession of the item.

Searches without consent must be carried out by the Headteacher or someone authorised by them. The person undertaking the search must be the same sex as the child being searched and the search must be witnessed by another staff member of the same sex. Intimate searches are prohibited and only outer clothing may be removed.

Staff may seize anything which reasonably believe is a prohibited item or is evidence in relation to an offence.

If inappropriate material is found on a device it is up to the teacher to decide whether they should delete that material or retain it as evidence of a criminal offence or a breach of school discipline. It should always be retained if an incident is sufficiently serious as to warrant police involvement.

Staff can dispose of pornographic images unless its possession is an offence (extreme, illegal or child pornography).

Images should NEVER be downloaded by staff as evidence; the act of downloading could be construed as a criminal offence in itself. Instead, staff should confiscate the phone and contact the police immediately.

Communication of Policy

Pupils

- Rules for internet access are posted through school.
- Pupils will be informed that use of the internet and computers is monitored.
- Policy is outlined at an age-appropriate level in the Codes of Conduct and reinforced through regular lessons.
- eSafety is a dedicated strand of the computing curriculum and as such is taught rigorously and progressively through school

Staff

- eSafety policy is covered in new staff induction and staff knowledge is refreshed and updated through regular training and messages.
- The AUA is read and signed by every staff member as a condition of employment and usage. A reminder appears onscreen each time they log in, and they must click to accept the terms. The AUA, updated by the eSafety Lead as required, must be re-read and re-signed at least every two years.
- Staff are aware that internet and computer use is monitored and can be traced to the individual user. High professional and personal standards are expected and this is also reinforced by the general Staff Code of Conduct.

Parents

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school brochure, on the school website and via the AUA.

Ratified by Governors on 14 July 2017

Signature of Chair of CPC Committee ……

Appendix A

Acceptable Use Agreements

Early Years Rules for IT
I will look after equipment.
I will only use the internet with an adult.
I will tell an adult straight away if I see something that I think is wrong or upsetting.
I will never tell strangers anything about myself.

Key Stage 1 IT Code of Conduct	
School equipment	I will look after IT equipment.
Logging in	I will only use my own user name to log in.
	I will not use any device under someone else's log in details.
	I will not tell anyone my password.
Staying safe online	I will only use the internet when an adult is nearby.
	I will not talk to strangers online or in real life.
	I will not take photographs of anybody else or put photos on the internet unless I have checked with a teacher.
	If I see anything that I think is wrong or upsetting, I will immediately close the lid of my device or turn it over.
	If I see anything that I think is wrong or upsetting, I will then tell a teacher.
	I will not share personal information online.
Behaviour	I will ask if I need help.
	I will always be polite on the internet.
Personal equipment	I will not bring any mobile device into school. This includes phones and disk drives.

I understand that if I break any of these rules the school will take the matter very seriously, and that school will take action which could include the following:

- The incident could be logged.
- My parents could be told.
- My use of the internet could be stopped for a length of time decided by the school.
- My use of IT devices could be stopped and my account suspended.

I understand that school filtering and monitoring software is installed and teachers can review what I do when I use school computers.

I understand the IT Code of Conduct and I promise to keep the rules.

Key Stage 2 IT Code of Conduct	
School equipment	I will look after IT equipment.
Logging in	I will only use my own user name to log in.
	I will not use any device under someone else's log in details.
	I will not tell anyone my password.
	I accept that I am responsible for all activity carried out under my user name.
Staying safe online	I will only use the internet when an adult is nearby.
	I will not talk to strangers online or in real life.
	I will not never arrange to meet anyone I have only met online.
	I will not take photographs of anybody else or put photos on the internet unless I have checked with a teacher.
	If I see anything that I think is wrong or upsetting, I will immediately close the lid of my device or turn it over.
	If I see anything that I think is wrong or upsetting, I will then tell a teacher.
	I will not share personal information online.
	When searching the internet, I will always use Safe Search.
	I will not download software or inappropriate files.
	I will never arrange to meet anyone I have only met online.
	I will not open emails or attachments from unknown senders.
Behaviour	I will ask if I need help.
	I will always be polite on the internet, including all posts on blogs, on social media, and in emails, texts and messages.

Personal equipment	I will not bring any mobile device into school. This includes phones and disk drives.

I understand that if I break any of these rules the school will take the matter very seriously, and that school will take action which could include the following:

- The incident could be logged.
- My parents could be told.
- My use of the internet could be stopped for a length of time decided by the school.
- My use of IT devices could be stopped and my account suspended.

I understand that school filtering and monitoring software is installed and teachers can review what I do when I use school computers.

I understand that although the internet and computer use seems private, it is not, and that anything I write or post could potentially be seen by many people.

I understand the IT Code of Conduct and I promise to keep the rules.

Parents

IT Acceptable Use Agreement

The national curriculum requires pupils to use IT, including computers and other devices, as an essential part of learning.

Pupils AND their parents/carers are asked to sign an Acceptable Use Agreement which outlines the rules and behavioural expectations. This is an important element of eSafeguarding and online safety.

It is intended to ensure:

- *that pupils use IT equipment, the internet and other communication technologies responsibly and safely;*
- *that school systems and other users are protected misuse, whether accidental or deliberate;*
- *that parents/carers are aware of the importance of eSafeguarding and are involved in the process of educating, protecting and guiding children.*

I give permission for my child to use school IT equipment, including accessing the internet.

I understand that my child will be taught about the safe use of such equipment and the internet, and will also be expected to sign an Acceptable Use Agreement (IT Code of Conduct).

This teaching will help them to understand the importance of the safe use of technology, mobile devices and the internet both in and out of school. I will support their learning by upholding high standards of eSafety at home. If I am unsure how to do this I will ask school staff and/or attend parent information sessions where safer online usage is explained.

I understand that my child may not bring devices into school. This includes – but is not restricted to - phones, tablet computers, disk drives and USB devices. These are classed as prohibited items in school.

I understand that school operates filtering and monitoring software to keep pupils' use of technology under constant active review, and that school will contact me if they have any concerns about breaches of the Acceptable Use Policy.

I will contact school if I have any concerns about my child's use of technologies and/or the internet, or if I become aware of any eSafeguarding problems in or out of school.

Acceptable Use Agreement: Staff, Visitors and Governors

ICT and the related equipment and technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. All staff must be aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Safeguarding Lead or the Headteacher.

1. I will only use electronic devices that are the property of Newby Primary School, the school's email, internet, intranet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by prior arrangement with the Head or Governing Body.
2. I will not disclose my initial login password or passcode to anyone.
3. I will always shut down or lock my computer/device when leaving it unsupervised by me.
4. I will ensure that all electronic communications with pupils and staff are compatible with my professional role, having reference to relevant Codes of Conduct, for example the published Staff Code of Conduct.
5. I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
6. I will only use the approved email system for any school business.
7. If sharing confidential information with another agency by email I will either remove names or use an encrypted service such as Egress Switch.
8. I will ensure that personal data (such as data held on SIMS or school reports) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I will only use encrypted computers, iPads or USB sticks for storing or editing personal data. (Note: iPads are encrypted by adding a pass lock.) Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. If a school device is lost or stolen whilst in my possession I will inform school immediately.
9. I will not install any hardware or software without permission of the IT Manager.
10. I will not use devices such as USB sticks and flash drives to upload files downloaded outside the protected environment of the school system.
11. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on a computer or device owned by Newby Primary School in or out of school, nor allow others to do so.
12. Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Such images must always be taken using school devices and never on personal devices. Images will not be distributed outside the school network without the permission of the relevant person.
13. I understand that all my use of the internet and other related technologies can be monitored and logged.
14. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
15. I will respect copyright and intellectual property rights.
16. I will do my best to ensure that my online presence will not bring me, my professional role, or the school into disrepute. In particular, I understand that I am accountable for any social media content relating to me or my activities both in and out of school. I understand that this means that I also have to be aware of what friends or others might publish about me.
17. I will support and promote online safety as described in the school's eSafeguarding policy and associated curriculum planning, thereby helping pupils to be safe and responsible in their use of ICT and related technologies.

For those employed on any basis by school, or hired through an agency: I understand this forms part of the terms and conditions set out in my contract of employment and that any breach of this agreement could result in disciplinary action being taken.

For those on a placement, such as for training or study purposes: I understand that any breach of this agreement could result in the termination of my placement.

For Governors: I understand that any breach of this agreement could result in referral to the School Governor Service.

Appendix B

Guidance on specific apps/games/social media platforms widely used by children at Newby (Feb 2017)

	Developer or PEGI rating	NSPCC Independent Panel Rating (where available) See www.net-aware.org.uk	
Grand Theft Auto	**18+**		Content PLUS online risks
Call of Duty	**18+**		Content PLUS online risks
WhatsApp	**16+**	**15+**	
Kik	**13+**	**15+**	
Snapchat	**13+**	**14+**	
Facebook	**13+**	**15+**	
Musical.ly	**12+**		Online risks
Tango	**13+**		
ooVoo	**13+**		
Rocket League	**8+**		Content suitable but option for online play

Nearly all social media and online interactive products carry risks of stranger contact and grooming. There is also however a very common risk of children 'getting it wrong' and either being perceived as bullying or becoming upset themselves about what is said, written or posted about them.

Some sites such as Tango and ooVoo carry heightened risks because they are 'public' by default, and strangers in the area of anyone using the app can freely connect with them.

Appendix C

Roles and Personnel 2017/18

Designated Safeguarding Lead: Claire Thompson

eSafety Governor: Elaine Palframan

eSafety Lead: Andy Ramsden

IT Curriculum Lead: Sarah Berry

Chair of IT Group: Gareth Baterip

IT Manager: Dianne Simpson

IT Technician: Andrew Kenworthy

Securus monitoring: Janice Stephenson on behalf of eSafety Lead