Normanby  Primary School

Ironstone Academy Trust

# Computing & Online Safety

Updated: January 2024

Author: Sonia Herlingshaw

At Normanby Primary school, we aim to deliver computing in a way which allows pupils to think creatively and promote independent learning behaviours by harnessing the power of technology as a learning tool. We maximise learning potential by creating confident, resilient digital citizens who have the transferable skills they need to be successful in an increasingly technology focused world.

Using technology to enhance learning does not stand-alone, it is an integral part of all learning across all subject areas. Our delivery and organisation of computing is in such a way that we do not exclusively restrict its use to a time or location but deliver the required skills 'at the point of learning,' where they become relevant and meaningful. Learners are therefore empowered to make choices about the relevance of the technology and apply it effectively.

Through direct teaching, and through experience gained in other curriculum areas, children develop their skills in the following areas:

1. Digital Literacy including Online Safety (Project Evolve)- the ability to communicate in a safe and respectful manner is a high priority in the teaching of Computing skills.

2. Information Technology including Digital Agency - we teach children to be creative in the way they use technology to communicate their knowledge and understanding of the world. We teach children how to use technology to expand their knowledge, while at the same time teaching them how to do so safely.

3. Computer Science including Programming - we teach children how to use technology to solve problems. Using arange of devices and software, we teach children the skills of problem solving, creativity and logical thinking which underpin the skills needed to program.

At Normanby, we endeavour to create a learning environment that maximises learning potential both inside and outside the classroom. Our children have 1:1 iPads from Y3 to Y6 which includes a Parental Contribution iPad Scheme and a 'Bring Your Own Device' (BYOD) Scheme. We have shared sets for KS1 and Foundation Stage children for use in school.

We strive to build the power of learning by creating classroom cultures that cultivate the habits and attitudes of curious, confident and independent learners. Unlocking learning behaviours and building learning habits that equip our young people with skills to thrive in the 21st Century.

**Contents** **Page**

# Aims and Values

The school's aims are to:

- Provide a relevant, challenging and enjoyable computing curriculum for all pupils.
- Meet the requirements of the national curriculum programmes of study for computing.
- Use computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.
- To equip pupils with the confidence and capability to use their computing skills and knowledge throughout their later life.
- To enhance learning in other areas of the curriculum using their understanding of computing.
- Provide efficiently for remote learning
- To develop the understanding of how to be safe and responsible users of technology.

The national curriculum for computing aims to ensure that all pupils:

- can understand and apply the fundamental principles of computer science, including logic, algorithms, data representation, and communication
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

# Rationale

*The school believes that computing:*

- *Gives pupils immediate access to a rich source of materials.*
- *Can present information in new ways which help pupils understand access and use it more readily.*
- *Can motivate and enthuse pupils.*
- *Develop problem solving, logical reasoning and computational understanding.*
- *Mold children into adept digital citizens, digital creators and digital communicators.*

# Objectives

**Early Years**

It is important in the EYFS (Early Years Foundation Stage) to give children a broad, play-based experience of Technology in a range of contexts, including outdoor play. Technology is not just about computers. Early years learning environments should feature Technology scenarios based on experience in the real world, such as in role play. Children gain confidence, physical skills and language skills through opportunities to 'paint' on the whiteboard, take & print photos using iPads or drive a remote-controlled toy. Outdoor exploration is an important aspect, supported by Technology toys such as metal detectors and walkie-talkie sets. Recording devices can help children to develop their communication skills.

**ELG (early learning goals) for the End of the Reception Year:**

- Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purpose.

**At the end of key stage 1 pupils should be taught to:**

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

**By the end of key stage 2 pupils should be taught to:**

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs, work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behavior; identify a range of ways to report concerns about content and contact

**Resources and Access to planning**

As the school develops its resources and expertise to deliver the computing curriculum, *objectives are* planned in line with the national curriculum and will allow for clear progression. *Projects* will be designed to enable pupils to achieve the stated objectives set outin the NC PoS for each key stage and the ELG. Pupil progress towards these objectives will be recorded by teachers as part of their class recording system.

**Assessment and record keeping (also see assessment policy)**

Teachers regularly assess capability through observations and looking at completed work. Key objectives in the programming strand are taken from the national curriculum to assess key computing skills each year and to track progress. Assessing computing work is an integral part of teaching and learning and central to good practice

**Monitoring and evaluation**

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching in line with the schools monitoring cycle. This may be through lesson observations, learning walks and feedback given from staff at standards meetings. The subject leader is also responsible for supporting colleagues in the teaching of computing, for being informed about current developments in the subject, and for providing a strategic lead and direction for the subject in the school. We allocate special time for the vital task of reviewing samples of children's work and for visiting classes to observe teaching in the subject.

**Remote Learning**

The schools remote learning offer is shared on the website and sets an expectation that we will provide a safe learning environment in which we will deliver a broad and balanced curriculum.

**Pupils with special educational needs (see also SEND policy)**

We believe that all children have the right to access computing. In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adapt

the delivery of the Computing curriculum. We teach computing to all children, whatever their ability. Computing forms part of the national curriculum to provide a broad and balanced education for all children. Through the teaching of computing, we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate computing can be used to support SEND children on a one-to-one basis where children receive additional support.

**Equal opportunities (see also equal opportunities policy)**

At Normanby Primary School we will ensure that all children are provided with the same learning opportunities regardless of social class, gender, culture, race, disability or learning difficulties. As a result, we hope to enable all children to develop positive attitudes towards others. All pupils have equal access to computing and all staff members follow the equal opportunities policy. Resources for SEND children will be made available to support and challenge appropriately.

## Role and Responsibilities

**Computing Subject Leader**

- There is a computing leader who is responsible for producing a computing development plan and for the implementation of the computing policy across the school.
- To offer help and support to all members of staff (including teaching assistants) in their teaching, planning and assessment of computing.
- To maintain resources and advise staff on the use of resources.
- To monitor classroom teaching or planning following the schools rolling programme of monitoring.
- To monitor the children's computing work, looking at samples of different abilities.
- To manage the computing budget.
- To lead staff training on new initiatives and update staff on changes.
- To attend appropriate in-service training and keep staff up to date with relevant information and developments.
- To have enthusiasm for computing and encourage staff to share this enthusiasm.
- To keep parents and governors informed on the implementation of computing inthe school.
- To liaise with all members of staff on how to reach and improve on agreed targets

- To help staff to use assessment to inform future planning.

**The role of the class teacher**

Individual teachers will be responsible for ensuring that pupils in their classes have opportunities for learning computing skills and using computing across the curriculum. The class teacher will also complete the computing assessments to tracker to identify any 'gaps', which need addressing.

**CPD**

**Staff training**

The computing subject leader will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year. Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the subject leader.

**Health and safety (see also health and safety policy)**

The school is aware of the health and safety issues involved in children's use of resources. All fixed electrical appliances in school are tested by a la contractor every five years and all portable electrical equipment in school is tested by an external contractor every twelve months. It is advised that staff should not bring their own electrical equipment into school but if this is necessary, then the equipment must be pat tested before being used in school. This also applies to any equipment brought into school by, for example, people running workshops, activities, etc. and it is the responsibility of the member of staff organizing the workshop, etc. to advise those people. All staff should visually check electrical equipment before they use it and take any damaged equipment out of use. Damaged equipment should then be reported to the senior sitetechnician, bursar or head teacher who will arrange for repair or disposal.

- Children should not put plugs into sockets or switch the sockets on.
- trailing leads should be made safe behind the equipment
- liquids must not be taken near the computers
- magnets must be kept away from all equipment

**Cross curricular links**

As a staff we are all aware that computing capability should be achieved through core and foundation subjects. Where appropriate, computing should be incorporated into schemes of work for all subjects. Computing should be used to support learning in other subjects as well as develop computing.

**Parental involvement**

Parents are encouraged to support the implementation of computing where possible by encouraging use of computing skills at home during home-learning tasks and through the school website. They will be made aware of online safety links and encouraged to promote this at home. We will create opportunities for parents to develop their knowledge in this field further with annual online safety training and drop-in sessions. 'Marvellous me' is an app used to consolidate learning, encourage and praise children and engage parents with their child's learning journey. This has been successfully rolled out across school and is a direct line of communication with parents.

# Normanby Primary School

## Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Normanby Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Normanby Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

## Policy development, monitoring and review

This Online Safety Policy has been developed by the *Online Safety Group* made up of:

- *Headteacher/Senior leaders*
- *Designated safeguarding lead (DSL)*
- *Online Safety Lead (OSL)*
- *Staff*
- *Governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

| | |
|---|---|
| This Online Safety Policy was approved by the *school governing body on:* | *May 2023* |
| The implementation of this Online Safety Policy will be monitored by: | *Mrs Herlingshaw OSL* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Annually* |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | *January 2025* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *Mrs Pentney Headteacher DSL*<br><br>*Mrs Brallisford Deputy Headteacher DSL* |

## Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *Spot check information*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *learners*
    - *parents and carers*
    - *staff.*

# Policy and leadership

## Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

## Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and deputy headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

## Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the governing body whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- *membership of the school Online Safety Group*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

## Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- meet with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

## Online Safety Lead (OSL)

The Online Safety Lead will:

- lead the Online Safety School Improvement Team
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

## Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding

  they have read, understood, and signed the staff acceptable use policy (AUP) **(Appendix 6 & 6a)**
-

- they immediately report any suspected misuse or problem to *Headteacher* for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

## IT Provider

The DfE Filtering and Monitoring Standards says:

> *"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."*
>
> *"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*
>
> *"The IT service provider should have technical responsibility for:*
>
> - *maintaining filtering and monitoring systems*
> - *providing filtering and monitoring reports*
> - *completing actions following concerns or checks to systems"*
>
> *"The IT service provider should work with the senior leadership team and DSL to:*
>
> - *procure systems*
> - *identify risk*
> - *carry out reviews*
> - *carry out checks"*

"We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to OneIT for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (Headteacher DHT and OSL receive alerts)
- *monitoring systems are implemented and regularly updated as agreed in school policies*

## Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- extending the level of filtering at school to outside school
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.

- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

*Parents and carers will be encouraged to support the school in:*

- *reinforcing the online safety messages provided to learners in school.*
- *the safe and responsible use of their children's personal devices in the school (where this is allowed)*

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- Online Safety Lead
- senior leaders
- online safety governor
- School Improvement Team
- technical staff
- teacher and support staff members
- learners - digital ambassadors

Members of the Online Safety Group will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

# Policy

## Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:

> "Online safety and the school or college's approach to it should be reflected in the child protection policy"

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (to be described)
- *is published on the school website.*

## Acceptable use

**The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.**

## Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- staff login screen
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- school website
- peer support.

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**<br>• Child sexual abuse imagery*<br>• Child sexual abuse/exploitation/grooming<br>• Terrorism<br>• Encouraging or assisting suicide<br>• Offences relating to sexual images i.e., revenge and extreme pornography<br>• Incitement to and threats of violence<br>• Hate crime<br>• Public order offences - harassment and stalking<br>• Drug-related offences<br>• Weapons / firearms offences<br>• Fraud and financial crime including money laundering<br>N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges | | | | | X |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission)<br>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to | | | | | X |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| | the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here | | | | | |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | X | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | Using school systems to run a private business | | | | X | |
| | Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school | | | | X | |
| | Infringing copyright | | | | X | |
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | X | X | |
| | Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| Consideration should be given for the following activities when undertaken for non-educational purposes:<br><br>Schools may wish to add further activities to this list. | Staff and other adults | | | | Learners | | | |
|---|---|---|---|---|---|---|---|---|
| | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awareness |
| Online gaming | ⊗ | | | | ⊗ | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Online shopping/commerce | | | ⊗ | | ⊗ | | | |
| File sharing | | ⊗ | | | | | ⊗ | |
| Social media | | | ⊗ | | ⊗ | | | |
| Messaging/chat | | | ⊗ | | ⊗ | | | |
| Entertainment streaming e.g. Netflix, Disney+ | | | ⊗ | | ⊗ | | | |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok | ⊗ | | | | ⊗ | | | |
| Mobile phones may be brought to school | | | ⊗ | | | | | ⊗ |
| Use of mobile phones for learning at school | ⊗ | | | | ⊗ | | | |
| Use of mobile phones in social time at school | | | ⊗ | | ⊗ | | | |
| Taking photos on mobile phones/cameras | ⊗ | | | | ⊗ | | | |
| Use of other personal devices, e.g. tablets, gaming devices | ⊗ | | | | ⊗ | | | |
| Use of personal e-mail in school, or on school network/wi-fi | | | ⊗ | | ⊗ | | | |
| Use of school e-mail for personal e-mails | ⊗ | | | | ⊗ | | | |

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*

- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

## Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

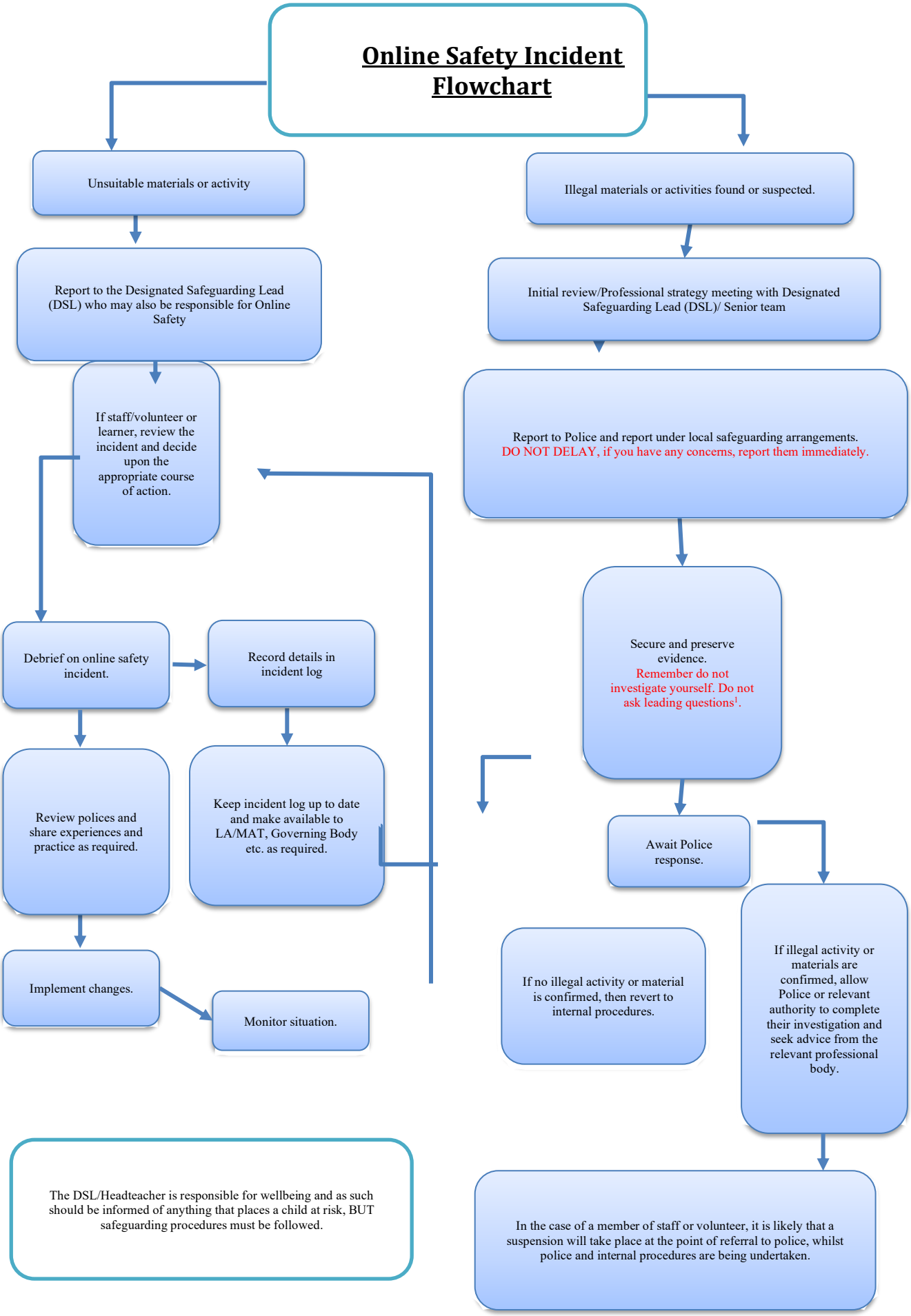
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the

content on the machine being used for investigation. These may be printed, signed, and attached to the form.

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / MAT (as relevant)
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged with DSL
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*
    - *parents/carers, through newsletters, school social media, website*
    - *governors, through regular safeguarding updates*
    - *local authority/external agencies, as relevant*
    -

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

## School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

## Responding to Learner Actions

| Incidents | Refer to class teacher/tutor | Refer to CEO | Refer to Headteacher | Refer to Policy | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Issue a warning | Further sanction, in line with behaviour policy |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities). | | X | X | X | | X | X | | |
| Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords | X | | X | X | | X | | X | X |
| Corrupting or destroying the data of other users. | | | X | X | | X | X | | X |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | X | | X | X | | X | X | | X |
| Unauthorised downloading or uploading of files or use of file sharing. | X | | X | X | | X | X | | X |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | X | | X | X | | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Accidentally accessing offensive or pornographic material and failing to report the incident. | | X | X | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material. | | X | X | | | | | | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. | X | | X | X | | X | X | | X |
| Unauthorised use of digital devices (including taking images) | X | | X | X | | X | X | | X |
| Unauthorised use of online services | X | | X | X | | X | X | | X |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | X | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions. | | X | X | | | | | | |

| Incidents | Refer to line manager | Refer to Headteacher/ Principal | Refer to local authority/MAT/HR | Refer to Police | Refer to Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)** | | X | X | X | | | | |
| Deliberate actions to breach data protection or network security rules. | | X | X | X | X | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | X | X | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | X | X | X | X | X |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | X | X | X | X | X |
| Unauthorised downloading or uploading of files or file sharing | | X | X | X | X | X | | |
| Breaching copyright or licensing regulations. | | X | X | X | X | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account. | | X | X | X | X | X | X | X |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | X | X | X | X | X |
| Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers | | X | X | X | X | X | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Inappropriate personal use of the digital technologies e.g. social media / personal e-mail | | X | X | X | X | X | | |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner | | X | X | X | X | X | | |
| Actions which could compromise the staff member's professional standing | | X | X | X | X | X | | |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | X | X | X | X | X | X |
| Failing to report incidents whether caused by deliberate or accidental actions | | X | X | X | X | X | | |
| Continued infringements of the above, following previous warnings or sanctions. | | X | X | X | X | X | X | X |

## Responding to Staff Actions

## Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following

A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.

- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.* Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through: (amend as relevant)

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors (or similar groups)*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital ambassadors leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

## Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- *the Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days*
- *the Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.*

## Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

## Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*

- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers*
- *Sharing good practice with other schools in clusters and or the local authority/MAT*

## Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- *providing family learning courses in use of digital technologies and online safety*
- *providing online safety information via their website and social media for the wider community*

# Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

## Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:
"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place …governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility. **The filtering and monitoring provision is reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.**

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice.

## Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- *School has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*
- *School has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

## Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.

- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

## Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in local authority / MAT / other relevant body policy and guidance):

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.

- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Computing Leader and Technician is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place and restrictions set for inside and outside school
- guest users are provided with appropriate access to school systems based on an identified risk profile.

## Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

| | **School devices** | | | **Personal devices** | | |
|---|---|---|---|---|---|---|
| | School owned for individual use | School owned for multiple users | Authorised device[2] | Student owned | Staff owned | Visitor owned |
| Allowed in school | **Yes** | **Yes** | **Yes** | Yes as part of BYOD scheme only | Yes | Yes |

[2] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

| | | | | | | |
|---|---|---|---|---|---|---|
| Full network access | Yes | Yes | Yes | Yes as part of BYOD scheme only | No | No |
| Internet only | | | | | | |
| No network access | | | | | | |

School owned/provided devices:

- *all school devices are managed though the use of Mobile Device Management software*
- *there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed*
- *personal use (e.g. online banking, shopping, social media, images, access to the app store etc.) is clearly defined and expectations are well-communicated.*
- *the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.*
- *liability for damage aligns with current school policy for the replacement of equipment.*
- *education is in place to support responsible use.*

## Personal devices:

- *there is a clear policy covering the use of personal mobile devices on school premises for all users*
- *where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.*
- *where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storge should be made available.*
- *use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems*
- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined*

- *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

## Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts

- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

## Twitter

Our School twitter is used as a tool to communicate with the world around us and craft our professional online identity. As ultimately anyone has the potential to create our online identity, we, as a school, want to manage our own online presence. Our school has multiple twitter accounts and staff are encouraged to create a class account with a professionalemail address, this should not be linked with any personal accounts and is entirely separate. All accounts are to be sanctioned by the Head teacher and monitored regularly. These accountsare managed by staff professionally and tweets reflect our school policies.
It is the account holder's professional responsibility not to approve tweets that would be deemed 'derogatory' for our school. Photo permissions are obtained for every child upon entry to school.

## Facebook

We recognised the large numbers of parents and carers using Facebook as their chosen means to communicate. Our rationale was to create a Normanby Primary schoolpage where parents and carers can share successes and selected information regarding events,notices and achievements. Photo permissions are obtained for every child upon entry to school.

Our Normanby Primary School Facebook page is professionally managed by staff and open to the Facebook community. Content from this page can be re-shared. It is not linked to any personal Facebook accounts and staff are not permitted to link to any personal account inconjunction with this account. This account is sanctioned by the Head teacher and monitored regularly.

## Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the school permits reasonable and appropriate access to personal social media sites during school hours*

## Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.

- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

## Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes unless senior leaders have approved the device and photos are deleted afterwards.
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images*
- *care should be taken when sharing digital/video images that learners are appropriately dressed*
- *learners must not take, use, share, publish or distribute images of others without their permission*

- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy*
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- *learners' work can only be published with the permission of the learner and parents/carers.*

## Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by Itchy Robot. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

*The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.*

## Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so

- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- has procedures in place to deal with the individual rights of the data subject,
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software

- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

**Appendices** **Page**

Appendix 1

Communications

| Communication Technologies | Staff & other adults | | | | Students/Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at a certain time | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| 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/personal devices or other camera devices not owned by school | | | | ✔ | | | | ✔ |
| Taking photos on mobile phones/personal devices or other camera devices owned by school | ✔ | | | | ✔ | | | |
| Use of handheld devices e.g., iPads | ✔ | | | | ✔ | | | |
| Use of personal email addresses in school, or on school network | | ✔ | | | | | | ✔ |
| Use of school email for personal emails | ✔ | | | | | | | ✔ |
| With e-safety Training and in a professional capacity only… | | | | | | | | |
| Use of chat rooms/facilities | | ✔ | | | | | ✔ | |
| Use of instant messaging | | ✔ | | | | | ✔ | |
| Use of social networking sites | | ✔ | | | | | ✔ | |
| Use of blogs | | ✔ | | | | | ✔ | |
| Marvellous Me | ✔ | | | | | | | |

Appendix 2

**Wireless Network SSID**

| **User** |
| --- |
| NPS (Normanby Primary School) Staff Wi-Fi |
| NPS Pupil Wi-Fi |
| NPS Guest Wi-Fi |

Any unauthenticated device internet is heavily filtered however devices can be assigned a static IP (Internet Protocol)address which would all the filtering to be more relaxed.

Any authenticated devices filtering will be based up the authenticated user groups.

Guest SSID is on a separate network which gives the device a 192 IP Address when connecting to the internet users will be asked to log in.

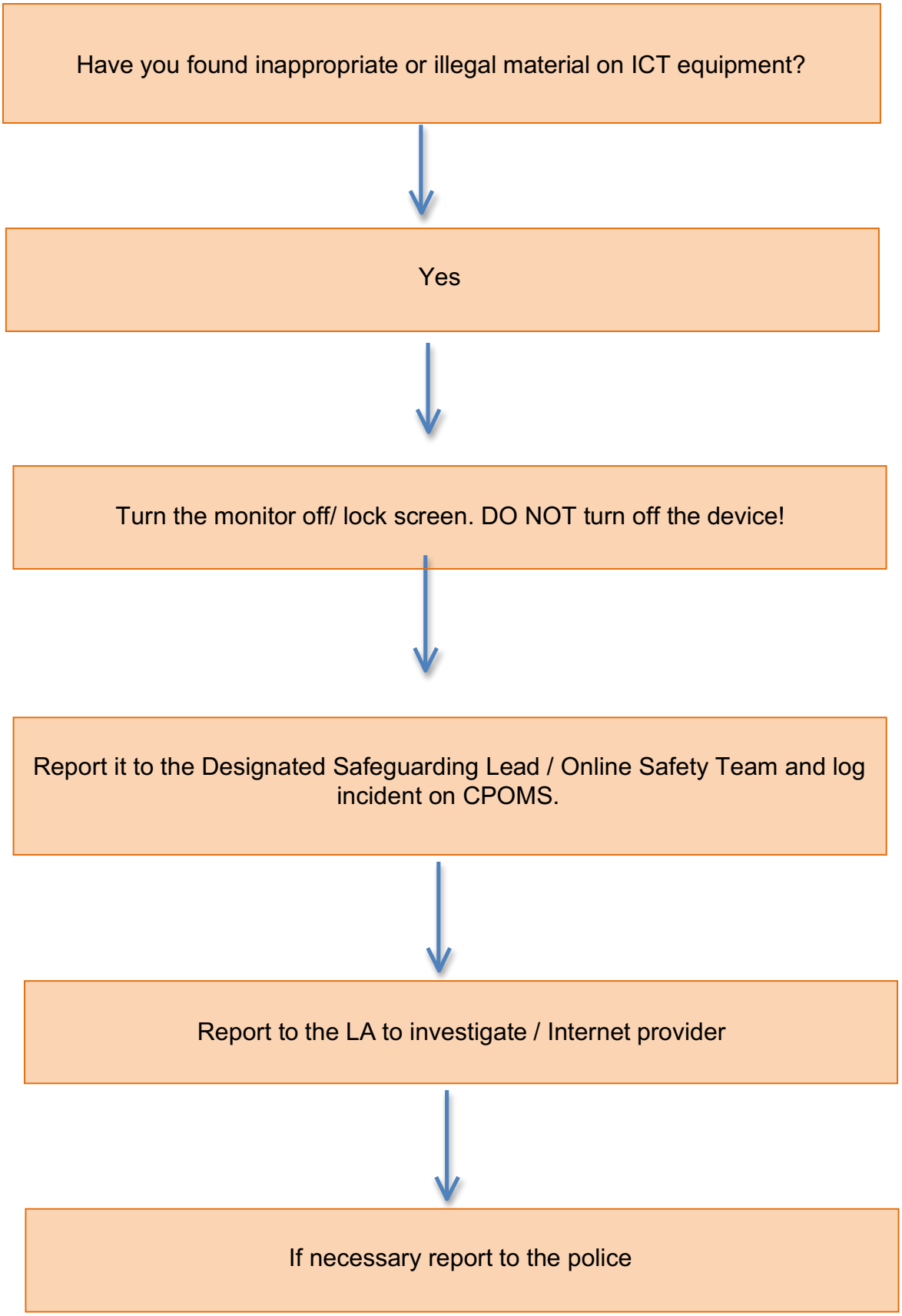
Appendix 2b
User Actions…

Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

| | Acceptable | Acceptable at certain times | Acceptable for nomination | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| Child sexual abuse images | | | | | ✔ |
| Promotion or conduct of illegal acts | | | | | ✔ |
| Adult material that potentially breaches the Obscene Publications Act in the UK | | | | | ✔ |
| Criminally racist material in the UK | | | | | ✔ |
| Pornography | | | | ✔ | |
| Promotion of any kind of discrimination | | | | ✔ | |
| Promotion of racial or religious hatred | | | | ✔ | |
| Threatening behavior, including promotion of 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 LA/school | | | | ✔ | |
| Uploading, downloading or transmitting commercial software ware or any copyrighted material belonging to third parties, without the necessary licensing permissions | | | | ✔ | |
| Revealing or publicising confidential or propriety information | | | | ✔ | |
| Creating or propagating computer viruses or other harmful files | | | | ✔ | |
| Carrying out sustained or instantaneous high-volume network traffic that causes network congestion and hinders others in their use of the Internet | | | | ✔ | |
| Online gaming (educational) | | | | ✔ | |
| Online gaming (non-educational) | | | | ✔ | |
| Online gambling | | | | ✔ | |
| On-line shopping/commerce e.g., fruit shop | ✔ | | | | |
| File sharing | ✔ | | | | |
| Use of social networking sites | ✔ | | | | |
| Use of video broadcasting with adult guidance e.g., YouTube | ✔ | | | | |

Appendix 3

## Responding to incidents of misuse/error



## Appendix 3b

Dear Staff,

As you are all aware we have a walled garden in school, which filters the websites which you and the children are allowed to access, for safety reasons. This system is not 100% guaranteed therefore we need to be aware of potential risks, for both children and adults.

There are procedures set out in the Online Safety policies in school to follow if such events arise. These are summarized below.

You need to:

- Immediately turn the screen off / put the device to sleep (pressing home/lock button)
- Leave the website on the computer/ device
- Report it to the Online Safety Team /HT immediately
- Log incident on CPOMS with required action and including appropriate staff
- If required, it will be investigated by our Internet provider
- If it needs to be then it will be reported to the police.

Just remember it is not yours or the children's fault, but it does need dealing with!

This procedure should be followed and children in all classes should be made aware of it.

Appendix 4

## Misuse of the Online Safety Policy

If you find you or another member of staff have possibly not abided by the Online Safety policy and rules have been breached, then please follow the following procedures to rectify the problem.

Seeking advice from the Online Safety Team
(Who will, if necessary, have an unofficial word with the Head Teacher)

Word of advice (reminder if it continues)

CONTINUAL ABUSE

Computing Leader will refer the matter to the Head Teacher

A meeting will take place with the Head Teacher and Computing Leader.
Minutes of the meeting taken and monitored

Formal investigation into continual abuse of the school policy

CONTINUAL ABUSE

LA (Local Authority) will be informed, and disciplinary proceedings will commence

.

# Acceptable Use Policy for iPads
# School iPad

- Your iPad will be linked to the school internet.
- Only use websites which you are directed to. (Don't go on inappropriate websites!)
- Always ask your parents / carers permission when linking your iPad to your home or any public network as responsibility for internet use outside school lies with them.
- I understand that school may check my files and monitor the internet sites I visit at school.
- Only go on the internet when the teacher asks you.
- Always ask permission before taking a photo or video of another person.
- Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.
- Always ask permission before changing any settings on your iPad.
- Charge your iPad every night ready for learning the next day.
- Always use the charger it came with.
- Bring your iPad to school every day, as it is a vital learning tool.
- Make sure you only take videos and photos in an appropriate setting (e.g. not in a bathroom, bedroom etc)
- School is silent! (turn your volume off in school).
- Always remember to take your iPad home on a night.
- Only ever touch your own iPad. Only touch other devices if you have permission.
- Personalise your own iPad, with a screen saver and wallpaper appropriate for school.
- Keep all documentation in a safe place at home.
- When you are not using your iPad lock it away in a safe place.
- Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).
- Always send polite and responsible messages, messages will be monitored.
- I understand social networking apps or websites are not permitted in school.
- I understand school will provide me with some key apps for my learning and I must not delete them, school also provides a more secure network for me to access the internet and other Wi-Fi networks.
- Always ask before downloading additional apps and make sure they are age appropriate.
- Always ask permission if linking your iPad with an Apple ID. (Parent or Carers may have details they don't want you to access).
- I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionally at school if teachers deem so.
- I understand that my iPad will be linked to schools mobile device manager system, school can see my device and what apps I am downloading and restrict content.
- I am clear that school retains the right to restrict any content deemed unsuitable.
- I understand that my device will use applications such as, but not limited to: Microsoft, Seesaw, Apple Classroom to enhance our learning experiences at home and school.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn't written above don't do it!
You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

| | | | |
|---|---|---|---|
| Child Name: | | Parent/ Carer Name: | |
| Signature: | | Parent/Carer Signature | |
| Date: | | Date: | |

Pupils, parents, carers, staff and governors all want Normanby Primary to be a safe and happy place, so that you can learn and enjoy your time at school. All of our policies reflect this and we all should use any item of equipment in a sensible, kind and thoughtful manner.

Normanby Primary School

# Acceptable Use Policy for iPads
# Scheme iPad

- Your iPad will be linked to the school internet.
- Only use websites which you are directed to. (Don't go on inappropriate websites!)
- Always ask your parents / carers permission when linking your iPad to your home or any public network as responsibility for internet use outside school lies with them.
- I understand that school may check my files and monitor the internet sites I visit at school.
- Only go on the internet when the teacher asks you.
- Always ask permission before taking a photo or video of another person.
- Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.
- Always ask permission before changing any settings on your iPad.
- Charge your iPad every night ready for learning the next day.
- Always use the charger it came with.
- Bring your iPad to school every day, as it is a vital learning tool.
- Make sure you only take videos and photos in an appropriate setting (e.g. not in a bathroom, bedroom etc)
- School is silent! (turn your volume off in school).
- Always remember to take your iPad home on a night.
- Only ever touch your own iPad. Only touch other devices if you have permission.
- Personalise your own iPad, with a screen saver and wallpaper appropriate for school.
- Keep all documentation in a safe place at home.
- When you are not using your iPad lock it away in a safe place.
- Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).
- Always send polite and responsible messages, messages will be monitored.
- I understand social networking apps or websites are not permitted in school.
- I understand school will provide me with some key apps for my learning and I must not delete them, school also provides a more secure network for me to access the internet and other Wi-Fi networks.
- Always ask before downloading additional apps and make sure they are age appropriate.
- Always ask permission if linking your iPad with an Apple ID. (Parent or Carers may have details they don't want you to access).
- I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionally at school if teachers deem so.
- I understand that my iPad will be linked to schools mobile device manager system, school can see my device and what apps I am downloading and restrict content.
- I am clear that school retains the right to restrict any content deemed unsuitable.
- I understand that my device will use applications such as, but not limited to: Microsoft, Seesaw, Apple Classroom to enhance our learning experiences at home and school.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn't written above don't do it!
You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

| | | | |
|---|---|---|---|
| Child Name: | | Parent/ Carer Name: | |
| Signature: | | Parent/Carer Signature | |
| Date: | | Date: | |

Pupils, parents, carers, staff and governors all want Normanby Primary to be a safe and happy place, so that you can learn and enjoy your time at school. All of our policies reflect this and we all should use any item of equipment in a sensible, kind and thoughtful manner.

Normanby Primary School

# Acceptable Use Policy for iPads
# Home iPad

- I understand at school my iPad will be linked to the school internet and monitored and filtered with our school systems.
- Only use websites which you are directed to. (Don't go on inappropriate websites!)
- I understand that school may check my files and monitor the internet sites I visit at school.
- Only go on the internet when the teacher asks you.
- Always ask permission before taking a photo or video of another person.
- Always make sure your iPad is out of reach when the teacher is talking to avoid fiddling.
- Always ask permission before changing any settings on your iPad.
- Charge your iPad every night ready for learning the next day.
- Always use the charger it came with.
- Bring your iPad to school every day, as it is a vital learning tool.
- Make sure you only take videos and photos in an appropriate setting (e.g. not in a bathroom, bedroom etc)
- School is silent! (turn your volume off in school)
- Always remember to take your iPad home on a night.
- Only ever touch your own iPad. Only touch other devices if you have permission.
- Personalise your own iPad, with a screen saver and wallpaper appropriate for school.
- Keep all documentation in a safe place at home.
- When you are not using your iPad put it away in a safe place.
- Do not behave in a way that will cause damage to your iPad. (Take care not to swing or drop your iPad).
- Always send polite and responsible messages, messages will be monitored.
- I understand school will provide me with some key apps for my learning and I must not delete them, school also provides a more secure network for me to access the internet than other wifi networks.
- The apps that are on my iPad are appropriate for my age and will not cause offensive to others.
- Always ask an adult before downloading additional apps and make sure they are age appropriate.
- I understand social networking apps or websites are not permitted in school.
- Always ask permission if linking your iPad with an Apple ID. (Parent or Carers may have details they don't want you to access).
- The content on my iPad (e.g. apps, photos, notes, internet history) will be appropriate and not cause offence.
- I understand that my iPad is covered under your own insurance plan and school cannot be responsible for any damage, loss or theft.
- I understand I may lose functionality on my iPad after a certain time at night. I may also lose functionally at school if teachers deem so.
- I understand my device will be linked to our school's mobile device management system and school can view content on the device as well as enforce restrictions.
- I am clear that school retains the right to restrict any content deemed unsuitable.
- I am aware that my device will need to be configured by school, which includes a full reset of the device.
- I understand that my device will use applications such as, but not limited to: Microsoft, Seesaw, Apple Classroom to enhance our learning experiences at home and school.

These are the steps you should follow when using your iPad, inside and outside of school. If it isn't written above don't do it!
You need to agree to follow these guidelines and those in our Internet and Computing Curriculum Policies, sign the form below.

| | | | |
|---|---|---|---|
| Child Name: | | Parent/ Carer Name: | |
| Signature: | | Parent/Carer Signature | |
| Date: | | Date: | |

Pupils, parents, carers, staff and governors all want Normanby Primary to be a safe and happy place, so that you can learn and enjoy your time at school. All of our policies reflect this and we all should use any item of equipment in a sensible, kind and thoughtful manner.

Normanby Primary School

Dear Parents and Carers,

If you would like to unlock the app store on your child's iPad, please read the following information carefully before signing below.

- I will monitor the content downloaded from the app store
- The school is NOT responsible for any cost incurred by in-app purchases and app costs.
- I will ensure no explicit / inappropriate content is downloaded *(at Home the iPads are NOT monitored or filtered and have FULL access to the Internet)*
- I acknowledge that the app store is unrestricted and school has no control over the content
- I understand that school retains the right to blacklist any apps
- I understand social networking apps are not permitted in school
- I will refer to the Apple terms and conditions when creating an apple id account
- Any issues/questions with your Apple ID must be directed to Apple as school has no control or visibility over it

Name of Child _____Class_____

I agree to the above information. I would like my child's iPad unlocking to give access to the app store.

Signed _____

# Terms and Conditions (Y3)

- I understand that whilst my child is at Normanby Primary School, I will make 36 monthly payments to EDDE for the iPad unless I paid in full via the portal.
- I understand the iPad is owned by school until the payments have been complete then ownership will transfer over to the parent.
- I understand that I can make two zero excess insurance claims within a 12 month period and my iPad is insured for 42 months.
- I understand that if my child leaves school before completing the 36 monthly payments, the iPad cannot be released to the child until all the remaining balance is paid. Any outstanding debt will be pursued.
- We reserve the right to retain the iPad if your account has arrears or if the iPad fails to be in school ready for learning.
- Linking the device with an apple ID, to download content from the app store, is the sole responsibility of the parent/carer. The apple store is unrestricted by school and content may not be suitable for child use. Your child must seek approval from the account holder before downloading any content.
- Upon leaving Normanby Primary School, we will revoke any apps purchased by school as these are owned by us.
- School retains the right to restrict any content deemed unsuitable but does not guarantee all unsuitable content will be blocked and responsibly of this is solely with the parent/carer.
- I understand school places a level of filtering on the use of the iPad in school and out of school which will restrict some inappropriate content. I understand that my role as a parent/carer is to monitor the iPad outside school hours.
- I acknowledge that my device will be linked with a mobile device manager to allow the device to by managed by school this may include restrictions which are deemed suitable.

**I accept and acknowledge the conditions.**

Name of child_____

securly FOR PARENTS

# Securly Parent Portal

## What is Securly?

Your child's school is partnering with Securly to provide an online student safety solution, and parents' email addresses are registered by the school. Weekly activity emails provide snapshots of your child's Internet use while on a school-owned or 1:1 scheme device.

*The emails you receive can help start conversations around various topics, including education, online safety, and peer pressure.*

## How do I set up my Parent Portal account?

Parents cannot register their own email with Securly. Your child's school must register your email. The school will give you an estimate of when you will receive your first email from Securly.

The email from Securly will read "Your Child _____'s Activity Report" in the subject line. Once open, either click on "go to my parent portal" or "sign up for Securly, it's free." Then, complete the checkboxes to be directed to the portal.

I give permission for Normanby Primary School to register my email:

**Name of child: _____**

| Name of parent/guardian | Email address: |
|---|---|
| | |

**Signed _____**

Appendix 6

**NORMANBY PRIMARY SCHOOL**
**Ironstone Academy Trust**
**Acceptable Internet Use Policy for Visitors**

***Remember that we use Information Communication Technology and the Internet for learning!***

- ✓ Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children's education, staff professional development or the broader aims of the school.
- ✓ I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or unprofessional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with the Trust Policy.
- ✓ Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
- ✓ I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on social media.
- ✓ Access must only be made via the user's authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
- ✓ Do not download, use or upload any material which is unsuitable for use within the school, or which compromises the security of the school network.
- ✓ Do not reveal or share any personal information or photographs about any member of the school, adult or child.
- ✓ Ensure that children using the Internet are supervised at all times.
- ✓ When using web sites in the classroom, always assess the web page before displaying it to children.
- ✓ Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
- ✓ I will use the 'cloud space' provided to store information that does not identify any children's personal details.
- ✓ I will not plug in any personal USB storage devices as they could infect our network with malicious software.
- ✓ I will only use encrypted school issued devices to store information and all devices much be password protected.
- ✓ Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
- ✓ If unsuitable material is accessed inadvertently, the school's IT Leader should be informed directly. Individual user's Internet access will be monitored, including websites visited and e-mail use.
- ✓ If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
- ✓ The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.

I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated, and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.

Name: Date:

Signed:

Appendix 6a

**NORMANBY PRIMARY SCHOOL**
**Ironstone Academy Trust**
**Acceptable Internet Use Policy for Staff**

***Remember that we use Information Communication Technology and the Internet for learning!***

- ✓ Use of ICT Equipment (including mobile devices) and the Internet must be appropriate to children's education, staff professional development or the broader aims of the school.
- ✓ I understand that as an employee of the Trust there are Terms and Conditions that apply to my employment. Abuse or un-professional use of school equipment, or internet service if forbidden. Disciplinary action will be taken in line with the Trust Policy.
- ✓ Access to social networking sites, chatrooms or user groups (other than for professional use agreed in advance with the Headteacher/ICT Leader) is forbidden.
- ✓ I understand it is my responsibly when using social networking sites to behave in a professional manner which reflects the values of our school. I understand that my responsibilities as an employee mean I should not condone inappropriate or illegal behaviours through my actions on social media.
- ✓ Access must only be made via the user's authorised account and password, which should not be given to anyone else. Staff will be held responsible for access under their user ID.
- ✓ Do not download, use or upload any material which is unsuitable for use within the school, or which compromises the security of the school network.
- ✓ Do not reveal or share any personal information or photographs about any member of the school, adult or child.
- ✓ Ensure that children using the Internet are supervised at all times.
- ✓ When using web sites in the classroom, always assess the web page before displaying it to children.
- ✓ Email communications opened and sent during the school day should be relevant to your teaching role and responsibilities.
- ✓ I will use the 'cloud space' provided to store information that does not identify any children's personal details.
- ✓ I will not plug in any personal USB storage devices as they could infect our network with malicious software.
- ✓ I will only use encrypted school issued devices to store information and all devices much be password protected.
- ✓ Material accessed via the Internet is not copyright free. Respect the copyright of information accessed via the Internet. Care must be exercised in using the web content and sources of material should be acknowledged.
- ✓ If unsuitable material is accessed inadvertently, the school's IT Leader should be informed directly. Individual user's Internet access will be monitored, including websites visited and e-mail use.
- ✓ If you see anything you are unhappy with or you receive messages you do not like, let the ICT Leader/Headteacher know immediately.
- ✓ The use of personal email accounts (on a school provided device) in school is permitted for occasional and unavoidable access, when children are not present. The use of a personal device when children are present is not permitted.

I acknowledge that my use of the Internet in school will comply with the above guidelines and that a breach of the guideline may be investigated, and subsequent disciplinary action could follow. Any variation to this agreement will be agreed with the Head Teacher or IT Leader in advance and in writing.

Name: Date:

Signed:

Appendix 6c

# Normanby Primary School Digital Image Consent

## Date and Event

Please sign below if you are intending to use a video camera, digital camera or any other recording device, including mobile phones to record images of the school performance on the date specified above.
Images can only be used on the understanding they are only viewed (used) in the home environment and not shared by digital or other means

*Any photographs taken at school events are for personal use only and we ask that they are not published online including on social networking sites such as Facebook. As you are aware we seek permission for online publication and not all parents agree to photographs being published online for a number of reasons including serious child protection concerns. As a school it is important that we fully respect the privacy of such pupils, and we thank you for your support in this.*

| Child: | Name: | Signature: | Intended device: |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Committing an Illegal Act - Did You Know?

**1**

Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

**2**

If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

**3**

Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

**4**

Showing anyone else illegal material that you have received **is an illegal act**

**5**

Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

**6**

Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material

**7**

**Within 4 simple steps you could easily break the law 4 times. Each is a serious offence**

**8**

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

**9**

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

**Never personally investigate**. If you open illegal content accidentally report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

Appendix 8
NPS Bi-annual Consent form

# Normanby Primary School Combined Bi-annual Consent Form

**Images and videos parental consent form**

This form explains the reasons why and how Normanby Primary School may use images and videos of your child. Please read the form thoroughly and outline your agreement as appropriate.

Why do we need your consent?
Normanby Primary School requests the consent of parents on a bi-annual basis to use images andvideos of their child for a variety of different purposes.
Without your consent, the school will not use images and videos of your child. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why do we use images and videos of your child?
Normanby Primary School uses images and videos of pupils as part of school displays to celebrate school life and pupils' achievements; to promote the school on social media and on the school's website; and for other publicity purposes in printed publications, such as newspapers.
Where the school uses images of individual pupils, the name of the pupil will not be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil will not be used to accompany the text.
If, for example, a pupil has won an award and their parents would like their name to be published alongside their image, separate consent will be obtained prior to this.
Normanby Primary School may take images or videos of individual pupils and groups of pupils to use on social media, the school website, in school prospectuses and other printed publications, such as a newsletter.

Who else uses images and videos of your child?
It is common that the school is visited by local media and press, who take images or videos of school events, such as sports days. Pupils will appear in these images and videos, and these may be published in local or national newspapers, or on approved websites.
Parents, carers and other visitors may attend school for a range of reasons. If photography is allowed at these events, the school will keep a register of individuals who choose to do so. School will give advice that these images are for personal use, and that images of other children must not beshared on social media.
The following organisations may use images and videos of your children:

- Evening Gazette
- BBC, ITV and other Television and Media Channels

Where any organisations other than those above intend to use images or videos of your child, additional consent will be sought before any image or video is used.
What are the conditions of use?

- This consent form is valid for the current 2018/2019 academic year and for the following year.
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.

- The school will not use the personal details or full names of any pupil in an image or video, on our website, in our school prospectuses or any other printed publications.
- The school will not include personal emails or postal addresses, telephone or fax numbers on images or videos on our website, in our school prospectuses or any other printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school may use group or class images or videos with general labels, e.g., 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e., it would not be suitable to display an image of a pupil in swimwear.
- The school will take class images of your child which are available to purchase annually.

# Parental consent form for receiving marketing material

This form explains the reasons why and how Normanby Primary School may send you marketing material. Please read the form thoroughly and outline your agreement as appropriate.

Why do we need your consent?

Normanby Primary School requests the consent of parents on a bi-annual basis to send them marketing material, e.g., flyers, from organisations associated with the school, such as the PTFA, Music Works, Tom Burke Academy, Simon Carson Sports School and Chris Nixon Music Services.Without your consent, the school will not send you any marketing material. Similarly, if there are only certain conditions under which you would like to receive marketing material, the school will abide by the conditions you outline in this form.

Why are we sending you marketing material?

Normanby Primary School uses marketing material to promote the events that are taking place at school, for example the summer fair. Events which raise money for the school are onlysuccessful if the school receives support from the parents of its pupils; therefore, we feel it is important to obtain your consent to send you promotional material.

You are under no obligation to respond to any marketing material, and we appreciate that it maynot always be feasible for you to do so. Through sending marketing material, our primary aim is to inform you of the events that are taking place during the school year and, if you wish to take part in them, how you can do so and to what benefit.

What are the conditions of use?

- This consent form is valid for the current 2018/19 academic year and the following year
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not send any marketing material to parents that has not already been consented to.
- The school will not share this list with any third parties without prior consent from parents.
- The school will not send any marketing material to parents if it is not already mentioned in this form.

# ICT acceptable use agreement for primary pupils

At Normanby Primary, pupils are expected to:

- Only use ICT on the school premises for studying purposes.
- Use the class or school e-mail address when sending or receiving emails.
- Only open email attachments from people known to them or people who the teachers have approved.
- Make sure ICT communication with other pupils and adults is polite and responsible.
- Be responsible for their behaviour while using ICT.
- Inform their class teacher of anything they see online which makes them feel uncomfortable.
- Understand that their use of ICT can be checked and that parents/carers will be contacted if a member of school staff is concerned about a pupil's e-safety.
- Be careful when using computer equipment and treat it with respect.
- Abide by the rules regarding bringing personal devices into school.
- Seek the advice of a teacher before downloading material.

Pupils will not:

- Try to bypass the internet settings and filtering system.
- Share passwords.
- Delete or open other people's files and documents.
- Use other people's accounts.
- Send any content which is unpleasant. If something like this is found, such as inappropriate images or the use of offensive language, pupils will report it to theirteacher.
- Share details of their name, phone number or address.
- Meet someone they have contacted online, unless it is part of a school project and/or a responsible adult is present.
- Upload images, sound, video or text content that could upset pupils, staff and others.
- Try to install software onto the school network.

Parents will:

- Support and uphold the school's rules regarding the use of school ICT systems.
- Understand the school is not liable for any damages arising from use of IT equipment and systems
- Act in accordance with the school's policy when using the internet in relation to the school, its employees and pupils.
- Only store and use images of pupils for school or private purposes, acting in line with the school's IT Policy, and not share images of other pupils on-line
- Understand that whilst the academy uses a combination of filtering and supervision to manage access to the internet and IT systems, that the academy ca is not held responsible for children accessing inappropriate materials/ the nature of all the content hosted on the internet

# Summary Code of Conduct and Home School Agreement

This Agreement should be read in conjunction with information on our website and does not replace our Policies

For children to achieve success at school it is important that parents, children and the school areable to work together, each party having an equally significant part to play in the partnership.

In order that this partnership can work effectively, each party must be supportive of the otherand committed to working in the best interest of all concerned.

**Normanby Primary School will endeavour to: -**

- Provide a caring, well-ordered and stimulating environment.
- Offer a broad and balanced curriculum to pupils of all abilities.
- Achieve high standards of work through encouraging all pupils to do their best at all times, feel proud of their achievements and enjoy being a valued member of the school.
- Encourage the children to behave appropriately at all times.
- Keep you informed about general school matters and about your child's progress, attitude and behaviour in particular.
- Be open and welcoming at all times and offer a variety of opportunities for you to become involved in the school community.

**Parents will endeavour to:**

- Ensure regular attendance, punctuality and appropriate dress.
- Notify the school if, for any reason, my child cannot attend.
- Help my child to take an interest in their work and sustain effort and achievement.
- Let the school know about any matters which may affect my child at school.
- Support and encourage my child with homework and other opportunities for home-learning.
- Encourage my child to follow the school's Rights and Responsibilities structure and Healthy School activities.

Parents and Carers should be aware that the school follows the system of Safeguarding and Child Protection detailed in 'Keeping Children Safe in Education' and by the Local SafeguardingBoard. This governs how we relate to other agencies, and this sets up the framework for how staffare trained and subsequently deliver their responsibilities.

**Refreshing your consent**

This form is valid for the entire academic year, 2018/19 – it will be updated on a bi-annual basis. Parents are required to fill in a new form for their child alternate academic years.
Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g., an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g., safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g., amending the provisions for which consent has been provided for new requirements for consent, e.g., an additional form of distributing marketing material
- Changes to school circumstances, e.g., if a new headteacher reviews how the school markets itself
- Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Head of School. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the Head of School. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent
Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing images or videos that were shared prior to withdrawal; however, the school will make a reasonable effort to remove images of the pupil where possible, e.g., images of the pupil on the school's website will be removed.
If you would like to withdraw your consent, you must submit your request in writing to the Head ofSchool.

| | |
|---|---|
| Name of parent/ carer completing this form | |
| Name of pupil: | |
| Year Group: | |

**Declaration**

I,_____(Name of parent), understand:

- Why my consent is required.
- The reasons why Normanby Primary School uses images and videos of my child.
- Which other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my requirements.
- The reasons why Normanby Primary School sends me marketing material.
- Which other organisations may send me marketing material.
- The conditions under which the school will send me marketing material.
- I have provided my consent above as appropriate, and the school will send marketing material in line with my requirements.
- Consent is refreshed on a bi-annual basis.
- I will be required to re-provide my consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the Head of School

Name of parent: _____

Signature: _____

Date: _____

If you have any questions regarding this form, please do not hesitate to contact the Head of School at School.

# Providing your consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criterion.

| I provide consent to: | Yes | No |
|---|---|---|
| Using images of my child on the school website. | | |
| Using videos of my child on the school website. | | |
| Using images of my child on social media, including the following:<br>• Twitter, Facebook | | |
| Using videos of my child on social media, including the following:<br>• Twitter, Facebook | | |
| The local media use images of my child to publicise school events and activities (only including the organisations outlined above). | | |
| The local media use videos of my child to publicise school events and activities (only including the organisations outlined above). | | |
| Using images of my child in marketing material, e.g., the school brochure and prospectus. | | |
| Sharing my child's data with a school-appointed external photography company for official school images. This includes the following:<br>• Name, Class, Roll number | | |

| I provide consent to: | Yes | No |
|---|---|---|
| Receiving marketing material via email. | | |
| Receiving marketing material in printed copy. | | |
| Receiving marketing material from the following organisations within the school:<br>• The PTFA, The governing board, The Leadership Team | | |
| Receiving marketing material from the third-party organisations, judged appropriate by the Head of School | | |
| Receiving marketing material via email from third parties. | | |
| Receiving marketing material in printed copy from third parties. | | |
| Receiving marketing material for the academic year 2018/19 and 2019/20 | | |

| I provide consent to: | Yes | No |
|---|---|---|
| Allow my child to use School and Cloud based systems to support learning, including email. | | |
| Allow my child to access the internet to support learning. | | |