



Online Safety



Policy

Review Date: April 2023

Next Review: April 2025



This policy is underpinned by our Church School Vision of Every Opportunity to Flourish, Live Well Together and Valued and Valuable' underpinned by our Christian values of Respect, Honesty, Courage, Love, Peace and Kindness and sets out how the school ensures they play their part in keeping children safe online. Safeguarding children in every aspect of their life is a responsibility we take very seriously and understand that risk that children may be exposed to in real life, can also happen in the virtual environment. We are aware that there are also additional risks that present themselves when children are online. This policy sets out how we aim to support our children to live well together online.

Teaching Online Safety in Schools (January 2023) states:

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positives and exciting opportunities, but also challenges and risks.

We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

This policy lays out how Newton on Trent Church of England Primary School achieves this for its pupils and families. The clear aims of the policy are:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and confident to deal with risks when faced with them is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.
- Lay out the expectations for curriculum coverage and provision to ensure that children learn about respectful, positive and healthy relationships and the effect of their online actions on others knowing how to recognise and display respectful behaviour online.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least every two years and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

At Newton on Trent Church of England Primary School this governor is **Jack Heaselden**.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our school. In other schools, the day-to-day management of this is often delegated to another member of staff, the Online Safety Officer, but at Newton on Trent the Headteacher is also the Online Safety Officer.

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body, parents.
- The designated online safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

Online Safety Officer-Headteacher

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise governing body on all Online safety matters.
- Engage with parents and the school community on Online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff – from ARK ICT Solutions Ltd

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
 - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
 - Any online safety technical solutions such as Internet filtering are operating correctly.
 - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Headteacher.
 - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in his/her absence to the Senior Leader. If you are unsure the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this online safety policy are fully understood.

- The online incident will also be recorded on CPOMS.

Appendix 1 and 5 outlines what to do should an incident occur and which authorities, if any, should be contacted.

All Students

The boundaries of use of ICT equipment and services in this school are given in the Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. The curriculum is designed to ensure the following learning opportunities are provided:

- How to evaluate what they see online.
- How to know when to question communication or information from an online source.
- To ensure children understand what acceptable and unacceptable behaviour looks like.
- To know that standards of acceptable behaviour and honesty are the same in real life as there are online. They should understand the importance of showing respect online.
- Children to be able to identify age appropriate online risks and make informed decisions of how to act.
- Children will be taught in line with our safeguarding policy, how to recognise a trusted adult and what to do when you need support.

Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Further information on the objectives taught in the curriculum can be found in our wider curriculum documents.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have access to the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and emails, and links on the school website, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Newton on Trent Church of England Primary School uses a range of devices including PCs, laptops and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use NetSweeper software to prevent unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Online Safety Officer and ICT Support are responsible for ensuring that the filtering is appropriate and that

any issues are brought to the attention of the Headteacher. Alternatives to NetSweeper, such as iBoss, are constantly being reviewed such that improved products are implemented if identified.

Email Filtering – we use Microsoft Office 365 AntiSpam Services software to prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Where sensitive data relating to school and it's pupils needs to be communicated via email, then the procedure for sending **secure email** must be followed at all times, as per Lincolnshire County Council policy.. Any emails sent with attached documents containing sensitive data must also be password protected, and the password given verbally to ensure that only the intended recipient of the email has access to the document.

Encryption – All staff laptops and desktops that hold personal data (as defined by the Data Protection Act 1998) are encrypted using Microsoft BitLocker Encrypted. In addition, all removable drives purchased and issued to staff are encrypted using BitLocker Encrypted. This ensures that no data leaves the school on an un-encrypted device. Any breach (i.e. loss/theft of devices such as laptops or memory sticks) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. (Note: Encryption does not mean password protected.)

School data should not be held on any device that is not owned by school (and therefore BitLocker encrypted). Staff should ensure that any school data (including photos) held (historically) on such devices (personal laptops or personal removable drives), is transferred to school devices, and the data then deleted from their personal devices.

Staff will be issued with a USB memory stick, and the deadline for the transfer and subsequent deletion of data as outlined above is September 2017.

Should a personal removable drive belonging to a member of staff, pupil, or visitor, be inserted into a school device, an installed programme will be activated to automatically BitLocker Encrypt the drive. This means it will no longer be accessible anywhere without a school password. For this reason, we do not allow personal removable drives to be used in our devices, unless they are owned by staff, specifically for school use only, do not contain any sensitive data (including photos) and not shared with anyone else.

Should a visitor require use of a laptop to make a presentation from an external drive, we will provide a school laptop specifically held for this purpose (which does not have BitLocker Encryption on it).

Passwords for laptops and desktops – all staff will be unable to access any school laptop or desktop without a unique username and password. Staff will be prompted to change their passwords every four weeks, with an extension to this period at the beginning of the summer holidays so that staff are not required to come into school to change their passwords in this period. Passwords will also be changed immediately if there has been a compromise.

Pupils have a class and a personal login for pupil laptops/desktops which will not be changed.

Passwords for iPads – all staff are required to have a 4 digit passcode on their staff iPad, which is unique and memorable. If you suspect that someone other than yourself knows your passcode, you are obliged to change it.

Pupil iPads all have the same 4 digit passcode.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated automatically when new virus definitions are available. ICT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All school machines are set up such that removable drives are automatically scanned for viruses before use.

Safe Use of ICT in school

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this onlinesafety policy and the Staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Pupils are permitted to use the school email system, under the supervision of their class teacher, and as such will be given their own email address. The email address will be made up of their first name and a two-figured number, e.g. john.bloggs@newton-on-trent.lincs.sch.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Social Media, use of Mobile Phones and Digital Photography Policy, and is reiterated for clarity. All parents must sign a photo/video release slip.

Social Networking – there are many social networking services available; Newton on Trent Church of England Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Newton on Trent Church of England Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Twitter
- Facebook

Both of these platforms are used as a professional forum and mirrors the expectations of pupil, staff and parent's behaviour of those in school. These platforms are used to updates and celebrate events and achievements in school and at home.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day of receiving knowledge of the incorrect upload.

Incidents - Any online safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Senior Leader. The online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log on CPOMS.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Newton on Trent Church of England Primary School will ensure staff are regularly trained and kept abreast of new guidelines, information and changes.

Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Online safety is taught at the start of every new academic year which will take account the key messages needed to stay safe online but will also be adapted for any new emerging risks that children could be exposed to. Within our PSHE scheme, Jigsaw, the following is covered: use of technology within healthy relationships; taking responsibility with technology use; technology safety; sexting online gaming; gambling; safer online communities; dangers of online grooming; smart internet safety rules; and cyberbullying is included in types of bullying.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

This policy is available for anybody to read on the Newton on Trent Church of England Primary School website; upon review all members of staff will sign as read and understood both the **Online safety policy** and the **Staff Acceptable Use Policy**. A copy of this policy and the **Pupil Acceptable Use Policy** will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Linked Policies and Documents

Acceptable use Policy

Safeguarding Children policy

PSHE Policy

Jigsaw Online Portal

Behaviour Policy

Computing Policy

Remote Learning Policy

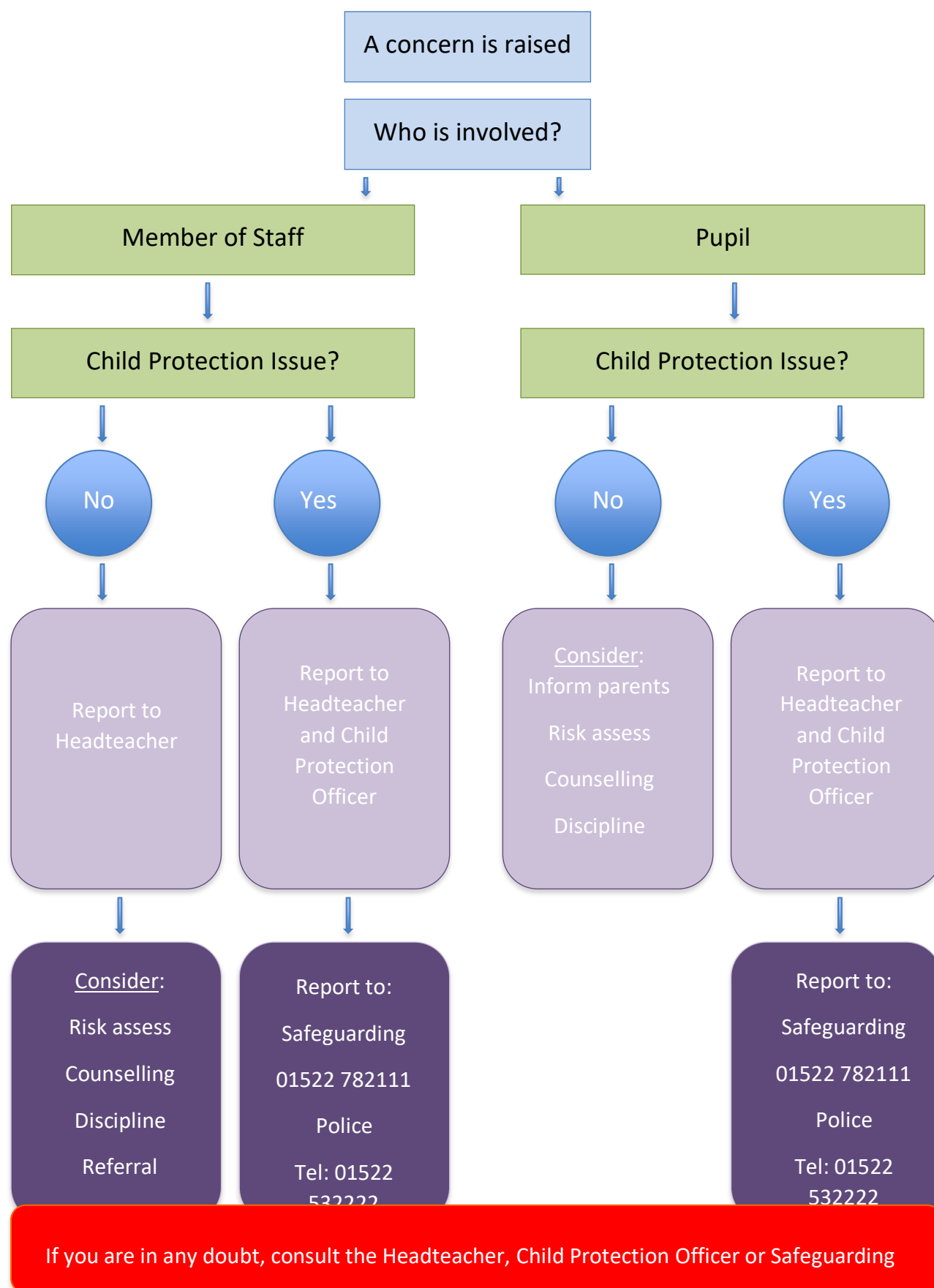
Relationships Sex and Health Education Policy

PSHE policy

Staff Code of Conduct

Guidance: Teaching Online Safety in School January 2023

Appendix 1 Inappropriate Activity Flowchart



Appendix 5

Illegal Activity Flowchart

