Newton Burgoland Primary School

E Safety Policy

Full copies of our policies and procedures can be found on our website or are available from the office www.newburland.leics.sch.uk

Adopted by the governing body at the meeting held in June 2018 – see minutes

Date of Implementation: 11/10/2017
Reviewed January 2019

To be reviewed annually.

Policy Statement

For clarity, the E-Safety Policy uses the following terms unless otherwise stated:

Users - refers to employees, governing body, school volunteers, pupils and any other person working in or on behalf of Newton Burgoland Primary School, including contractors.

Parent – any adult with a legal responsibility for the child/young person outside Newton Burgoland Primary School e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – student teachers, all employees, governing body, parents/guardians, parent helpers, visitors to school.

Safeguarding is a serious matter; at Newton Burgoland Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free 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.

This policy is available for anybody to read on the School website; upon review all members of employees will sign as read and understood both the E-Safety policy and the Employees Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils to be returned signed by parents and pupils; a copy of the policy is available to read on the school website and will be included in the new starter packs. Upon return of the signed policy and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet. A reminder of the policy will be sent home each year.

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 annually and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-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 E-Safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Head Teacher has overall responsibility for E-Safety within our school. The day-to-day management of this is shared with all members of employees.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all employees, senior leadership team and governing body, parents.
- All E-Safety incidents are dealt with promptly and appropriately.

All Employees will:

- Report any E-Safety concerns
- Attend training
- Promote safety with pupils and parents
- Supervise pupils when they are using the internet

ICT Technical Support Contractor - Kelvin Finch (Finch IT Solutions Ltd)

Finch IT Solutions Ltd (ICT Technical Support Contractor) 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 E-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 E-Safety officer and Head Teacher.
    - The administrator password is known only by the Head Teacher and ICT support. It will be changed whenever there is doubt that it has been breached - it is kept in a sealed envelope in the safe. Safe key holders are password holders.

All Employees are to ensure that:

- Teacher laptops are password protected and are changed whenever there is doubt that it may have been breached. Recommended Passwords- Use a minimum password length of 8 or more characters if permitted. Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.
- Sensitive data is not kept on laptops and is always encrypted or stored on a secured server drive.
- Teacher Ipads are pass-number protected and are changed whenever there is doubt that it may have been breached
- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any E-Safety incident is reported to the school business manager (and an E-Safety Incident report is made), or in his/her absence to the Headteacher. .
- The reporting flowcharts contained within this E-Safety policy are fully understood.

All Pupils

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

E-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by employees. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents, Guardians & Carers (Parents)

Parents play the most important role in the development of their children; as such the school will endeavor to ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. This will be done through parents evenings, school newsletters, and E-Safety events. The school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that pupils 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 student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

The school expects parents and families to abide by age guidelines and to supervise pupil internet access.

Pupils should not use mobile phones, tablets or computers unsupervised in bedrooms.

Technology

Newton Burgoland Primary School uses a range of devices including PCs, laptops, iPads and digital cameras. In order to safeguard our pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use AVG Cloud Care & Avast Business Antivirus filtering software that prevents unauthorized 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 ICT Coordinator, E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher. Our pupil iPads also run a child friendly browser instead of Safari. The browser is a high security browser that operates a strict filtering system on all websites accessed, recommended and installed by Finch IT Solutions Ltd (ICT Technical Support Contractor).

Email Filtering – we use Office 365 Business software that prevents any infected email being sent from the school or being 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 e.g. spam email such as a phishing message. Emails which include inappropriate language are blocked.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) 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.

Passwords – all employees and pupils will be unable to access password protected ICT equipment without the correct username and password..

Anti-Virus – All capable devices will have anti-virus software. This software will automatically update when new virus definitions become available. ICT Support will verify this has taken place correctly and any issues in the meantime will be reported to the office immediately.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to employees upon signing this E-Safety and the employees Acceptable Use Policy, and granted to pupils upon signing and returning their acceptance of the Pupil Acceptable Use Policy. See Appendix for exemplar Acceptable Use Policies.

Email – All employees 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.

Photos and Videos –All parents must sign a Photograph Consent Form on entry to school; non-return of the permission slip will not be assumed as acceptance. Notices of pupils without photographic permission are located in all school areas and trip folders Photos may be used on the school blog at www.newtonburgoland.primaryblogger.co.uk if consent is given on the form. When it needed, 'No Photograph' pupils will wear an armband to enable them to be easily identified.

Social Networking Pupils – All pupils at Newton Burgoland Primary School are under the legal age for using Social Media accounts such as Facebook, Instagram, and Twitter and therefore school does not condone the usage of these accounts. However, if it comes to our attention that pupils are using such accounts we will inform parents/guardians and offer safeguarding information, E-Safety education and support; a record of disclosure will be kept. The only social media used within school for educational purposes is the school blog- see above.

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

- Photograph Consent Forms must be consulted before any image or video of any child is uploaded. Notices of pupils without photographic permission are located in all school areas and trip folders.
- 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". A school-based moderator will approve comments before they appear on the blog.
- 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 license which allows for such use (i.e. creative commons).

Social Media – Adults in School
Adults in school will read and adhere to the Social Media Policy

Notice and Take Down Policy – should it come to the schools 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.

Incidents - Any E-Safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Head Teacher or Business Manager. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log. An exemplar incident log can be found in the Appendix. Also included in the appendix are example flowcharts, detailing how various E-Safety incidents should be dealt with.

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. E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, employees will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. This is done through age-appropriate, relevant resources that engage pupils and build upon their existing learning habits to help them become safe, responsible Digital Citizens. As well as our programme of training we will establish further training or lessons as necessary in response to any incidents.

The current E-Safety Training Programme can be found on the Employees Share drive.

Monitoring

All Internet usage at Newton Burgoland Primary School is monitored. This is to ensure that pupils and employees are:

1. Using the Internet appropriately, in accordance with the Employees and Pupil policies outlined in this E-Safety Policy.
2. Protected adequately by the filtering systems implemented with the intention of keeping pupils and employees safe.
3. Protected from inappropriate content that is harmful, distressing and otherwise inappropriate for a school setting.

All employees, pupils and parents of pupils will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites. All parents are made aware of this monitoring and are required to fill in a Monitoring Consent letter which can be found in the Appendix.

Data Protection

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Our Data Protection policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. In addition, the policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

Appendices: -

Acceptable Use Policy; Employees (including LA employees on site), trainees, governors, volunteers

Acceptable Use Policy; Pupils

Monitoring Consent Letter; Parents/Guardians

E-Safety Incident Log

Innappropriate Activity Flowchart

Illegal Activity Flowchart

Linked To:

Data Protection Policy

Social Media Policy

Camera's and Mobile Phones in School Policy

Safeguarding and Child Protection Policy

Keeping Children Safe in Education DFE

Newton Burgoland Primary School

Acceptable Use Policy – Employees (including LA employees on site), Governors, Trainees, Volunteers, Visitors, Contractors

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety Policy & Data Protection Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an E-Safety incident, reported to the E-Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the E-Safety policy only. Adults using social networking for personal use should never undermine the school, its employees, parents or children and must adhere to the Social Media Policy. Adults in school should not become "friends" with parents or pupils on personal social networks

Use of Email – employees are not permitted to use school email addresses for personal business. All email should be kept professional. Employees are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Employees should keep passwords private. There is no occasion when a password needs to be shared with another member of employees or student**.** Recommended Passwords- Use a minimum password length of 8 or more characters if permitted. Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.

Data Protection – the Data Protection Policy must be adhered to.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service, images or videos of yourself, other employees or pupils without consent. This is applicable professionally (in school) or personally (i.e. employees outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support.

Viruses and other malware - any virus outbreaks are to be reported to the Local Authority Helpdesk/ Finch IT Solutions Ltd as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, E-Safety is the responsibility of everyone to everyone. As such you will promote positive E-Safety messages in all use of ICT whether you are with other members of employees or with pupils.

I have read, understand and agree to adhere to the E-Safety Policy, the Acceptable Use Policy and the Data Protection Policy.

NAME :……

SIGNATURE :…….. DATE :……..

Newton Burgoland Primary School

Acceptable Use Policy – Pupils

"Our E-Safety Promises"

Note: All Internet and email activity is subject to monitoring

This policy has been written in collaboration with pupils from our school.

I Promise – to only use the school ICT for appropriate activities at appropriate times, as instructed by a member of staff.

I Promise – not to look for or show other people things that may be upsetting or are otherwise inappropriate.

I Promise – to show respect for the work that other people have done.

I will not – use, change or delete other people's files without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will not – use school equipment to save personal files not related to school.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – sensibly alert an adult if I encounter anything inappropriate when using the Internet in school.

I will – be respectful to everybody online: I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be unkind. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – that if I break the rules in this policy there will be consequences of my actions and my parents/guardians will be told.

Signed (Parent) :……

Signed (Student) :……..

Date : ……

Newton Burgoland Primary School

Monitoring Consent Letter- Parents.

Dear Parents/Guardians,

Use of the Internet in school is a vital part of the education of your child. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact the School Office to make an appointment to discuss the matter further.

Yours Sincerely,

Mrs Sue Ward- Head Teacher

I have read this letter and understand that my child's Internet access may be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –…….

Name of Child –…….

Signature - ……. Date: ……..

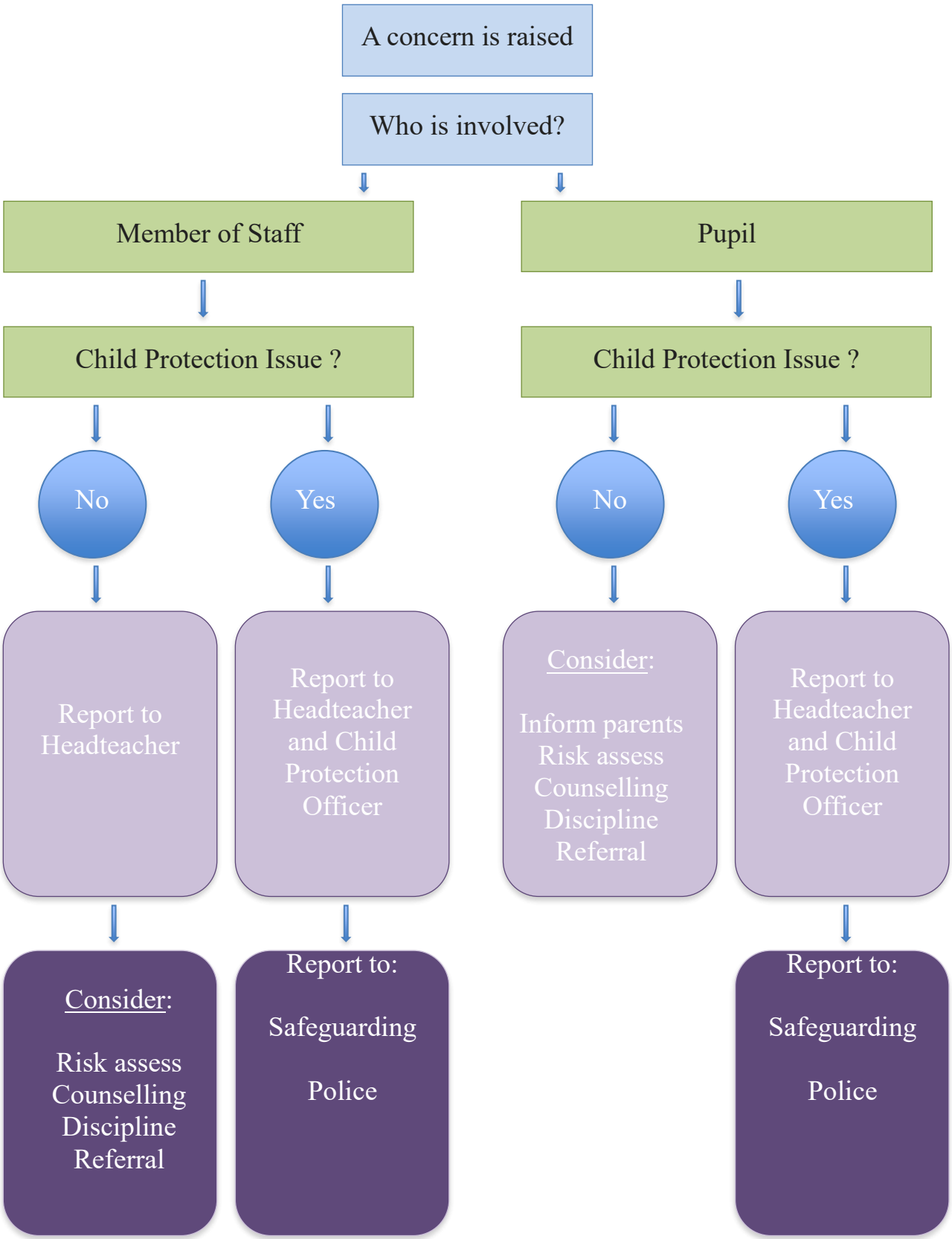
Newton Burgoland Primary School

E-Safety Incident Log

Reported By: *(name of employee/or other school community member)*	**Reported To:** *(E-Safety officer, HT, Business Manager)*
Incident Date:	
Incident Description: (Describe what happened, involving which children and/or employees, and what action was taken)	
Review Date:	
Result of Review:	

Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Innappropriate Activity Flowchart



Illegal Activity Flowchart