Permission form for ongoing Parental Consent*

Forename	Surname	Class	Address	Tel. No

Name of Parent/Guardian:

I declare that I am the legal parent or guardian of the above child.
I have read the attached information and give consent for my child to be included in the following activity(ies):

- Internet Access
- Copyright permission
- Data exchange
- Sex Education (age-appropriate within the science curriculum)
- Viewing appropriately selected films/clips

Photographs

☐ I give permission for my child's photograph or video image to be used for school and curriculum purposes, including Class Dojo. I understand that it may also be used for displays and for promoting a positive image of the school on the school website, in newsletters, press releases, newspaper articles, our social media, etc. and that my child's name will not be included in published images.

☐ I give permission for my child's image to be used in a group photograph what will be made available for sale only, to parents of children in that group.

☐ I do not give permission for photographs to be taken of my child.

(Please tick as appropriate)

Medical Consent

☐ I give my consent to the school, in the event that it is necessary, obtaining or rendering properly qualified medical assistance to my son/daughter. This consent will only be used where it is impossible to contact you.

Additionally,

☐ I hereby give my consent to my child's participation in any out of school activity in connection with work being done in class. I understand that this covers short, off-site visits where no charge is involved. I understand that a separate permission slip will be requested of me for any trip where a charge is involved, or where transport is necessary.

Signed:	Date:

***Please note that this consent form will be kept on file over the course of your child's time at school. If anything changes, please inform the school.**

Use of Internet and e-mail in school

As part of their work in Information Technology and other subjects, we offer the children supervised access to the internet and **internal** e-mail. On some occasions children are offered the opportunity to use e-mail outside the school, for example to communicate with children from other schools.

The internet is a rich source of information and educational activities which are of great benefit to the children. However, there are concerns about inappropriate materials and the school takes a range of measures to minimise these risks:

- All access to the internet is supervised by adults.
- A high level filtering system is in operation. This allows access only to children's search engines
- Children are not allowed access to chat rooms at any time
- Children are taught about safe internet use by their teachers.

Please see below an extract from the ICT and Internet Acceptable use Policy (including Cyber Security). The full policy can be found on the school website under Statutory Information – Policies.

Before we allow children to use the internet at school, parents **must** sign the permission form for Ongoing Parental Consent as evidence of their acceptance of the school's rules for responsible use of these facilities.

ICT and Internet Acceptable use Policy (Extract)

6. Pupils

6.1 Access to ICT facilities

Laptops, Ipads, netbooks and computers in the school's ICT suite are available to pupils only under the supervision of staff.

6.2 Searching, confiscation and deletion

Under the Education Act 2011, The Head Teacher, Assistant Head Teacher and senior members of staff have a statutory power to search pupils or their possessions, without consent, and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting has a harmful or detrimental to school discipline:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Searching with consent - Schools' common law powers to search:

School staff can search pupils **with their consent for** any item which is banned by the school rules.

1. The school does not need to have formal written consent from the pupil/parent for this sort of search – it is enough for the teacher to ask the pupil to turn out his or her pockets or if the teacher can look in the pupil's bag and for the pupil to agree.
2. Items which are banned in school include, mobile phones, electronic games or devices.
3. If a member of staff suspects a pupil has a banned item in his/her possession, they can instruct the pupil to turn out his or her pockets or bag and if the pupil refuses, the teacher can apply an appropriate punishment as set out in the school's behaviour policy.

4. A pupil refusing to co-operate with such a search raises the same kind of issues as where a pupil refuses to stop any other unacceptable behaviour when instructed by a member of staff – in such circumstances, schools can apply an appropriate disciplinary penalty.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting behaviour which is suspected to be harmful or detrimental they should:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher / SLT
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation if the pupil refuses to co-operate, we proceed according to the Behaviour and Relationship Policy.
- The authorised staff member should:
- Inform the Designated Safeguarding Lead (DSL) or deputy of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour and Relationship Policy, Appendix 2.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the Head Teacher / SLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- Our Behaviour and Relationship policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

10.1 Pupils Internet access

- WIFI is available across the school for pupils to use for educational purposes on school devices
- Filtering of these devices is through Wave 9 and the Sophos firewall
- Pupils are not allowed to access the school's WIFI on personal devices.

Pupil Acceptable Use Statement for – Parent Information

Digital technologies, including mobile phones and devices which can access the internet, have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone, and the can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school's **ICT and Internet Acceptable Use Policy** is intended to ensure the following:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As your child is a member Battling Brook Community they will be expected to follow our ICT guidance and rules, and as part of their ICT lesson and our commitment to e-safety, the school will have discussed the Acceptable Use Statement with them.

All children's activity on the ICT systems will be monitored, and we take every reasonable precaution through filtering, to ensure that young people will be safe when they use the internet and ICT system. However the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

We ask all parents/carers to encourage their child to adopt safe use of the internet and digital technologies at home and to inform the school if they have any concerns over their child's e-safety.

The school will contact parents/carers if they have concerns about any possible breaches of the Acceptable Use Statement.

The ICT and Internet Acceptable Use Policy (including Cyber Security) is available on the School Website: https://www.bbrook.leics.sch.uk

Pupil Acceptable Use Statement for EYFS and KS1

This is how I stay safe when I use computers:

- I will keep my passwords secret.
- I will only use the computer for things my teacher has told me to.
- I will make sure that all the messages I send are polite.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).
- In school, I will only use my school email. I will only email people I know or who my teacher says it is okay to email.
- I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.

Pupil Acceptable Use Statement for KS2

At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others.

- I will keep my passwords for login in to any computer or application to myself – if I think others know my passwords I shall tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school.
- I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
- If the computer asks for an update, I shall check this with my teacher.
- I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules I might not be allowed to use a compute

Watching films/Shorts/Clips

Over the course of an academic year we are likely to show shorts and clips from films to support teaching and learning. These may include carefully selected films/clips rated PG and below. All films will be suitable for the age range of the children and will have been checked by teachers to make sure they are appropriate for the children in each particular class.

Using Images of Children

From time to time our school may be visited by the media who will take photos or film footage, for example a visiting dignitary or other high profile event. Pupils often appear in these images which may then be published in newspapers or televised news programmes. We may take photographs of the children in school for displays in classrooms and around school, for the notice boards or for our school website. We may also make video or webcam recordings for in-class work, for working with our partner schools or other educational use. To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please complete the permission form as required

Battling Brook Privacy notice – pupil data

Introduction

As a school we collect a significant amount of information about our pupils. This notice explains why we collect the information, how we use it, the type of information we collect and our lawful reasons to do so.

Why do we collect data?

We collect and use pupil data to:

- fulfil our statutory obligations to safeguard and protect children and vulnerable people
- enable targeted, personalised learning for pupils
- manage behaviour and effective discipline
- monitor our effectiveness
- comply with our legal obligations to share data
- support pupils to fulfil their potential
- keep pupils, parents and carers informed about school events and school news

Our legal obligations

We must make sure that information we collect and use about pupils is in line with the UK GDPR and Data Protection Act 2018. This means that we must have a lawful reason to collect the data, and that if we share that with another organisation or individual, we must have a legal basis to do so.
The lawful basis for schools to collect information comes from a variety of sources, such as the Education Act 1996, Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013, Article 6 and Article 9 of the UK GDPR.
The Department for Education (DfE) and Local Authorities (LA) require us to collect certain information and report back to them. This is called a 'public task' and is recognised in law as it is necessary to provide the information.
We also have obligations to collect data about children who are at risk of suffering harm, and to share that with other agencies who have a responsibility to safeguard children, such as the police and social care.
We also share information about pupils who may need or have an Education Health and Care Plan (or Statement of Special Educational Needs). Medical teams have access to some information about pupils, either by agreement or because the law says we must share that information, for example school nurses may visit the school.

Sharing information

Other services, organisations and people we may share information with include:

- schools or academies that the students attend after leaving us
- relevant local authority/(ies)
- the Department for Education (DfE)
- the NHS as required
- school nursing service
- parent/carer
- suppliers and service providers
- health professionals
- health & social welfare organisations
- professional bodies
- charities and voluntary organisations
- auditors
- survey & research organisations
- social care organisations
- police forces and court services
- suppliers of software and apps that are used in the school

We must keep up to date information about parents and carers for emergency contacts.

How we use the data

In school we also use various third-party tools to make sure that pupils' best interests are advanced. We also record details about progress, attainment and pupil development to support future planning and learning.

We use data to manage and monitor pastoral needs and attendance/absences so that suitable strategies can be planned if required.

We use systems to take electronic payments for school meals. This includes financial software to manage school budgets, which may include some pupil data. We use software to track progress and attainment.

Data can be used to monitor school effectiveness, the impact of intervention and learning styles across groups of pupils as well as individual children.

We may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share pupil information with them if this is relevant to their work.

We also use contact information to keep pupils, parents, carers up to date about school events.

What type of data is collected?

The DfE and government requires us to collect a lot of data by law, so that they can monitor and support schools and academies more widely, as well as checking on individual schools and academies effectiveness.

The categories of pupil information that the school collects, holds and shares include the following:

- personal information – e.g. names, dates of births, pupil numbers and addresses
- characteristics – e.g. ethnicity, vulnerability categories, language, nationality, country of birth and free school meal eligibility
- attendance information – e.g. number of absences and absence reasons
- assessment information – e.g. national curriculum assessment results
- relevant medical information and social care
- information relating to SEND and health needs
- behavioural information – e.g. number of temporary exclusions
- CCTV, photos and video recordings

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools/academies in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the department. It is held in

electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

Immunisations and Vaccinations
The Department for Education has issued new guidance since December 2023 explaining that schools must share information with the School Age Immunisation Services (SAIS), who are commissioned by NHS England to deliver school-based immunisation programmes. Information that is to be shared on request includes a list of eligible children and young people and their parent or carer's contact details to the SAIS team.
The immunisation process is a matter of consent between the pupil, parent and or carer and the SAIS provider. The school do not take any active role in the process. The obligation to share data is within public task and does not rely upon consent. It is mandatory for the school to share this information.

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Laura Lyons (Data Protection Lead)
You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact

If you would like to discuss anything in this privacy notice, please contact Laura Lyons, the School Business Manager.

More information about data protection and our policies

How we manage the data and our responsibilities to look after and share data is explained in our data protection policy, and connected policies, which are also available on our website.
If you feel that data about your child is not accurate, or no longer needed please contact the school office. Our complaints policy explains what to do if there is a dispute. Subject Access Requests are dealt with by the specific policy on the website.

Review

The school will update this privacy notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.