

At Lobley Hill Primary School we aim to ‘Be the best that we can be’ through being curious, adventurous and respectful in order to achieve personal excellence.



Lobley Hill Primary School

Acceptable Use Policy

Approved by:	Governing Body	Date: October 2024
Last reviewed on:	October 2024	
Next review due by:	October 2025	

Computing Acceptable Use Policy

Introduction

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and trainees and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials
- Educational and cultural exchanges between pupils worldwide
- Access to experts in many fields
- Staff professional development such as access to online learning and forums
- Communication with support services, professional associations and colleagues
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

Internet use and access in Lobley Hill Primary School is considered a privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined below, will be imposed.

It is envisaged that staff and a governor will revise the AUP annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

General Internet use and Consent

Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Parent's/carer's permission to use their children's photographs on the website, in promotional materials and on social media will be sought at the beginning of each year. It is the responsibility of office staff to keep this information up to date and the responsibility of individual staff members to check before using any images. If a picture is placed on the website the child's full name will not be displayed.

Pupils must not use the school computing facilities without the supervision of a member of staff. Although use of the computing facilities and access to the Internet will be supervised, and all possible measures will be taken Lobley Hill Primary School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff, trainees or pupils discover unsuitable sites, the URL (address) and content must be reported to the IT Assist immediately who will, in turn, record the address and report on to the ICT co-ordinator and Internet Service Provider. In addition, filtering and monitoring reports will be sent daily to the School Business Manager identifying any potential inappropriate internet access. The school's filtering and monitoring is provided by SENSO and Netsweeper through IT Assist. The pupils will be issued with their own log in details in order to ascertain who has accessed the unsuitable sites on the internet.

Pupils are aware that they must only access those services they have been given permission to use.

Staff, trainees and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)

Staff, trainees and Governors must agree to and sign the Acceptable Use Agreement (appendix) each year.

Log in and Passwords

Staff and pupils must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.

Staff-and pupils must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

Staff and pupils must ensure desktops, ipads, laptops and programmes are logged off (or locked) when left unattended.

Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user. We recommend that passwords are changed frequently. Passwords should be over 8 characters and should contain letters, numbers and symbols. They should not contain spaces.

To protect your work area do not tell anyone your password. The password is displayed on screen as a line of *****, however people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful. Anyone who needs assistance in changing their password should contact the ICT technician (IT Assist).

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is potentially hazardous to both the equipment and to individuals.

Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Risk assessments are completed for use of iPads, iPad trolleys, laptops and laptop trolleys and are kept in the secure suite. Staff are responsible for sharing the safety issues with their pupils.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe computing practice into all our teaching and learning, incidents can be avoided.

We recognise we have a shared responsibility to prevent incidents of cyber bullying but the e-safety officer together with the Head Teacher has the responsibility for co-ordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has.

Staff receive guidance and school staff review the Anti-Bullying and Acceptable Use Policies annually. Children are taught how to recognise cyber bullying and their responsibilities to use computers safely. Computer safety is integral to teaching and learning practice in the school.

Parents are also taught how to recognise cyber bullying and their responsibilities for supporting safe computing during annual e-safety meetings and information leaflets throughout the year.

The school runs a regular computing lessons, PHSE lessons and assemblies focusing on cyber bullying and e-safety.

Record Keeping and Monitoring Safe Practice

As with other forms of bullying, the Headteacher keeps records of Cyber Bullying. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying.

E-Safety

Staff and pupils are reminded of the Acceptable Use Policy at the start of each term. The start of each computing session will be based on e-safety. Every year, parent/child e-safety sessions will be led in school. E-safety guidance will also be handed out throughout the year to ensure parents are aware of the importance.

Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden on the school network, with the exception of Leadership ipads (where it is used to update school sites).

Staff and pupils do not give personal email or postal addresses, telephone of any person.

Under no circumstances do staff and pupils give email or postal addresses / telephone numbers/fax numbers of any teachers or pupils at school to members of the general public.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

Users should assume that ALL software is subject to copyright restrictions, including shareware. Staff, trainees and pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff and trainees should seek the advice of the ICT technician (Omnicom) or the ICT Co-ordinator before attempting to download or upload software.

Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, homophobic or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or Computing lead. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

Social Networking

Staff need to be aware of the risks involved with social media and social networking sites. If staff are members of any social networking site, they are reminded of the necessity to keep their profiles secure and to avoid unnecessary contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil, staff confidentiality will be classed as a disciplinary matter.

The school Facebook site is used as a form of communication for parents and is operated by the School Business Manager and Admin Assistant. All parents are given the opportunity to state whether they would

like their child's photograph to go onto social media sites. Prior to any post checks must be made against the list of children's names for permission to be allowed on social media. Staff are able to be part of the Facebook site, however they must ensure that their profile is private and any comments that are made are appropriate. Any action on the social media account will be monitored closely.

It is unacceptable for pupils attending Lobley Hill Primary School to be members of Social Networking sites. The majority of Social Networking Sites have a minimum age limit of 13. The children of Lobley Hill Primary School do not meet this minimum requirement. We look to parents and carers to support the school with this ethos. Please refer to Guidelines for the Use of Social Media (P16-19).

Gaming

Children accessing online games in school will only do so with the direct support and supervision of a member of staff. Such gaming activity will be relevant, planned for and provide progression in learning. Children accessing online games at home are at risk due to other gamers misrepresenting themselves and gaining information about the child. Parents and carers experiencing difficulties at home will be supported by the Computing Lead and referred to http://www.thinkuknow.co.uk/8_10/control/gaming/.

School Network and Pupil Files

Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first (unless there is reasonable question over the content of the files). Files to be shared should be saved to the Staff Shared Area (Q:). Pupils can access and save work to their own log-on through the server; this can only be accessed by that child and the ICT technician (IT Assist).

Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.

The ICT technician (IT Assist) will view any material pupils store on the school's computers, or on memory sticks/disks pupils use on the school's computers.

Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Hard drives are provided for each Key Stage to store any important documents from previous years. Users unsure of what can be safely deleted should ask their teacher or ICT technician (IT Assist) for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician (IT Assist).

Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.

Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Security Guidelines

Backups

Files stored on the network are backed up regularly by IT Assist. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. (See above)

Home Documents

The school cannot accept responsibility for personal documents held on school laptops, it is the responsibility of the user to backup documents created at home or stored on the Home Docs of the laptop.

Offsite pupil data and pupil information

Staff should sign an agreement and this AUP at the beginning of the academic year which will allow them to take their staff iPad offsite, these iPads will be password protected but staff are responsible for ensuring that they are used cautiously and stored in a safe place whilst offsite. Backups (USB sticks) may be taken off site. Backups to hold pupil data or images should be in the form of encrypted USB pens, if any member of staff is unsure of how to do this, they should seek support from the ICT technician (IT Assist) or the Computing lead. Staff are to ensure that laptops are used cautiously when viewing pupil data/information and images and that laptops are logged off when left unattended. Images must be transferred to the school network as soon as possible to be removed within the set timescales. Data, images and pupil information must be removed from backups and laptops when pupils transfer to another class to avoid records being kept of pupils that are not taught by their former teacher.

Virus Checks

All computers in school have antivirus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician (IT Assist) using work log protocols.

E-Mail Usage

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer

When using e-mail, pupils and staff should:

- Be aware that e-mail is not a secure form of communication and therefore pupils should not send ANY personal information.
- Should not attach large files
- Must not forward e-mail messages onto others unless the sender's permission is first obtained.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated
- Must not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.
- Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated

This Guidance will apply to any inter-computer transaction, be it through web services, chat rooms,

Mobile Devices

With the exception of Year 6 pupils who walk home alone, pupils are not permitted to bring mobile phones or devices in to school. Should there be extenuating circumstances, which mean there is a need for a child to bring their device in to school, this should be turned off and handed to the School Office to look after during the school day and collected at 3.30pm.

Pupils may not make personal calls from a mobile phone during the school day.

Mobile phones may not be used to take pictures of pupils and staff (use class ipads provided by the school)

Pupils should not send or receive email or text messages to/from their mobile device during the school day.

Any inappropriate use of mobile devices such as cyber bullying must be reported to the Head Teacher (see Cyber bullying)

Staff should only use their own mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices

or cameras to take images of pupils or staff. The Headteacher reserves the right to request to view any photographs stored on mobile devices brought into school.

Any pupil who is seen with a mobile device during the school day will have it removed from them to be collected at the end of the school day (in accordance with the school's Behaviour Policy). The device will be secured in a safe location.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a mobile device and ipad.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT technician (IT Assist) to discuss the situation. Solutions are possible! Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Head Teacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at anytime. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

“Hacking” is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Further Support & Guidance

Websites linking to e-safety and Acceptable Use:

<http://www.thinkuknow.co.uk/>

<http://www.ceop.police.uk/>

<https://saferinternet.org.uk/>

Sanctions

If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Managing Allegations against Adults Who Work With Children and Young People

In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we will be referred to Gateshead LA. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Designated Safeguarding Leads the school immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Data Breaches should be recorded on the appropriate proforma and passed on to the Headteacher/responsible governor. This should include reporting personal incidents as well as reporting observed incidents.

Named Personnel

The Person Responsible for E-Safety and Acceptable Use is Rachel Hocking (Headteacher)

Guidelines for the Use of Social Media

Please refer to Social Media Policy

We were informed by our legal department that permission is not required for us to post or publish photographs of the children however best practice, courtesy and in line with our safeguarding responsibilities, it was advisable to seek parental permission. In terms of preventing others from taking photographs we have no legal rights to prevent this on or off school property as every parent has the right to photograph their own child, but we are able to request that this doesn't happen or that photographs are not posted in the public domain.

The aim of using social media is to enhance communication with parents and carers, to compliment our school website and run in conjunction with traditional communication such as letters.

Once agreed the following rationale and guidance for using Social media will be shared with staff and incorporated into our Acceptable Use Policy. Until this time, posting on any form of social media or internet site will not occur.

Rationale for the Use of Social media

- To improve and enhance communication with parents and carers
- To share events, activities and projects undertaken in school
- To share the achievements of the children in and out of school
- To enable families to share achievements with the wider family
- To promote Lobley Hill Primary School as the heart of the local community
- To model to children the benefits and positive impact social media can have
- To model best practice in line with safeguarding when using social media
- To provide a forum for parents and carers to raise queries, questions or minor concerns through the private messenger service
- To distribute (not receive) information

Guidance for the Use of Social Media –Meta

- A rationale will be sent to all parents/carers regarding the appropriate use of Social Media together with an explanation in regards to its intended purpose
- All school social media will be open to all followers however, we reserve the right to block accounts deemed inappropriate or offensive to ourselves and/or others
- We will not actively seek to follow other account users unless there is a direct impact and benefit to school
- New followers will be monitored by Headteacher to ensure they have a legitimate connection to Lobley Hill Primary School
- Login and password details will be kept secure by Headteacher
- Photographs of children are not be published or posted without parental consent
- No child currently in the Adoption, LAC or Child Protection system will be posted
- Any parent/carers undergoing assessment in relation to safeguarding or child protection will be removed from the page

- In order to promote the recommended guidelines suggesting an age limit of 13, children under this age will be blocked from the page
- Children's surnames will not to be posted (if a certificate is posted the name must be obscured)
- Events occurring outside of school will not to be published prior to occurring – there will be at least a 24 hour time lapse
- Only the designated staff (SBM/Admin Assistant) will post, publish and upload content in order to ensure safeguarding procedures are followed and only children with permission are posted and to monitor the content of posts
- A comprehensive list of all children with and without permission will be held by the school office and each staff member to ensure that when posts etc are being created only photographs of children with consent are being used
- No child (regardless of whether they have consent to have their photograph posted or not) will be excluded from any activity within school
- Reminders of events occurring within school will be posted
- All posts, content will be posted in a professional manner with constant regard being given to how it will reflect upon and represent school
- When posting residential updates, information will be generic, location will not be identified
- A maximum of 50 images will be uploaded linked to any one singular event or post
- A termly reminder will be posted to remind parents/carers and families the purpose and rationale behind the use of Facebook to ensure we limit any negative comments
- All comments on photographs and posts will be monitored and approved by Headteacher – these come directly via email initially before they are published
- Followers will not be able to tag themselves or others in photographs
- School information will only be posted on the official school site and not on the personal pages of any staff member
- Security of the school page will be checked regularly by Headteacher
- Any inappropriate content or comments will be removed immediately and the owner of such comments removed, banned and blocked from accessing the page and reported to Facebook. These include but are not exclusive to the following:
 - Offensive language or comments aimed at the school, its staff, parents, children, governors or anyone else affiliated with school
 - Unsuitable images or content posted into our feed
 - Unsuitable images or contents from another's account finding its way into our feed
 - Images or text that infringe copyright or lead to legal implications
 - Comments that undermine the school, its staff, parents, governors or others affiliated with school
 - *(A list of unacceptable and/or offensive words will be added to the security setting to further prevent misuse)*

Guidance for the Use of Social Media

- A rationale will be sent to all parents/carers regarding the appropriate use of Social Media together with an explanation in regards to its intended purpose
- All school social media will be open to all followers however, we reserve the right to block accounts deemed inappropriate or offensive to ourselves and/or others
- We will not actively seek to follow other account users unless there is a direct impact and benefit to school
- In order to promote the recommended guidelines suggesting an age limit of 13, children under this age will be blocked from the page
- All staff share the same login and password details – they will ensure these are kept securely
- New followers will be monitored by Headteacher to ensure they have a legitimate connection to Lobley Hill Primary School
- Photographs of children’s work may be posted but this will not contain any reference to children’s surname
- Events occurring outside of school will not to be published prior to occurring – there will be at least a 24 hour time lapse
- When posting residential updates, information will be generic, location will not be identified
- Security of the school account will be checked regularly by Headteacher
- Any inappropriate content or comments will be removed immediately and the owner of such comments removed, banned and blocked from accessing the page and reported to Twitter. These include but are not exclusive to the following:
 - Offensive language or comments aimed at the school, its staff, parents, children, governors or anyone else affiliated with school
 - Unsuitable images or content posted into our feed
 - Unsuitable images or contents from another’s account finding its way into our feed
 - Images or text that infringe copyright or lead to legal implications
 - Comments that undermine the school, its staff, parents, governors or others affiliated with school
 - *(A list of unacceptable and/or offensive words will be added to the security setting to further prevent misuse)*

Acceptable Use Agreement for Staff, trainees and Governors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to obtain permission for children and young people before they can upload images (video or photographs) to the internet or send them via email.
- I know that images should not be inappropriate or reveal any personal information of children and young people.
- I have read the procedures for incidents of misuse in the Lobley Hill Primary School Computing Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the e-safety officer in accordance with procedures listed in the Acceptable Use Policy.
- I know who my e-safety officer (computing lead) is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e-mail address and phones to contact parents.
- I know that I must not use the school system for personal use unless this has been agreed by the Head Teacher.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Head Teacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been shown a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow. A copy can be found on the school website.
- **I have read the additional information in regards to Social Media**

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Signed.....Date.....

Name (printed).....

Reporting Breach of Acceptable Use Policy

Incident Details:			
Date:		Member of staff/pupil name:	
Type of Breach: (e.g. non-secured devices, lost data storage, inappropriate use of social media)			
Reported to:		Position in school:	
Incident Severity and Outcome:			
Risk Grading A:		Risk Grading B:	
Consequence of the Breach 1 = None 2 = Minor 3 = Moderate 4 = Major 5 = Catastrophic		Likelihood of Recurrence: 1 = Cannot believe this will ever happen again 2 = Don't expect it to happen again but is possible 3 = May occur occasionally 4 = Will occur but not persistently 5 = Will undoubtedly occur, possibly frequently.	
Actual impact of Breach:		Action taken to avoid future recurrence:	
Details of person reporting the incident: Signed: Name:		Shared with Governor Responsible: Signed: Name:	