Tudor Grange Academies Trust

E-SAFETY POLICY

1. RATIONALE

Tudor Grange Academies Trust and all Academies within the Trust are committed to a policy of protecting the students in our care in line with the law. The use of the Internet and connected devices poses a risk to the safety of the young people in our care and this needs to be assessed and dealt with in line with other policies and the law of the land.

2. ASSOCIATED ACADEMY POLICIES

- Safeguarding Policy
- Acceptable Use Agreements
- Health and Safety Policy
- Procedures for Using Pupils' Images
- Behaviour Policy

3. COMPLIANCE

This policy applies to all governors/trustees, staff and students of Tudor Grange Academies Trust. Any breach of this policy, or of the Act itself will be considered an offence and the Academies disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with Tudor Grange Academies Trust, and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments or individuals who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

Teaching and learning

1. Why is Internet use important?

Internet use is part of the statutory curriculum and a necessary tool for learning.

The Internet is a part of everyday life for education, business and social interaction. The Academy has a duty to provide students with quality Internet access as part of their learning experience.

Students use the Internet widely outside Academy and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

2. How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of Academies, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with TGAW and examination bodies and the Department of Education.

Managing Information Systems

1. How will information systems security be maintained?

- The security of the Academy information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Academy computer activity will be monitored through Impero and reports checked regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the Academy's network will be regularly checked.
- The network manager will review system capacity regularly.

2. How will email be managed?

Students may only use approved email accounts.

Students must immediately tell a teacher if they receive offensive email.

Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

Access whilst in the Academy to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.

The forwarding of chain messages is not permitted.

Academies may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team.

Staff should only use Academy email accounts to communicate with students as approved by the Senior Leadership Team.

Staff should not use personal email accounts during Academy hours or for professional purposes

3. How will published content be managed?

The contact details on the website should be the Academy address, email and telephone number. Staff or students' personal information must not be published.

Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT'.

The website should comply with the Academy's guidelines for publications including respect for intellectual property rights and copyright.

4. Can student's images or work be published?

Images that include students will be selected carefully and will not provide material that could be reused.

Students' full names will not be used anywhere on the website, particularly in association with photographs.

Written permission from parents or carers will be obtained before images of students are electronically published.

Student work will generally be restricted to the Virtual Learning Environment which will only be accessed by staff and students of the Academy. Exceptional work may be displayed on the public website. Again, images of the student concerned would need permission from the parents.

5. How will social networking, social media and personal publishing be managed?

The Academy will control access to social media and social networking sites. The Academy does understand the need for a social network as Academy is a place of social learning. Academy based social networks may be used, but access will be restricted to staff and students only. These will be provided through the learning platform and e-portfolio systems.

Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples of personal details would include real name, address, mobile or landline phone numbers, Academy attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

Staff official blogs or wikis should be password protected and run from the Academy website with approval from the Senior Leadership Team. Staff should be advised not to run social network spaces for student use on a personal basis.

If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by Academy staff.

Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

6. How will filtering be managed?

The Academy will work with partner Academies to ensure that systems to protect students are reviewed and improved.

If staff or students discover unsuitable sites, the URL must be reported to TG IT Services.

The Academy's broadband access will include filtering appropriate to the age and maturity of students.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the Academy believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

The Academy's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

7. How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the Academy Website.
- The equipment must be secure and if necessary locked away when not in use.
- Academy videoconferencing equipment should not be taken off Academy premises without permission.

Users

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the students' age.
- Parents and carers should agree for their children to take part in videoconferences, probably in the annual return.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-Academy site it is important to check that they are delivering material that is appropriate for your class.

8. How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed.
- Staff will be issued with a Academy phone where contact with students is required.
- Mobile phones will not be used during lessons or formal Academy time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- The Academy should investigate wireless, infrared and Bluetooth communication technologies and decide a policy on phone use in Academy.

9. How should personal data be protected?

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. No personal data will be taken off Academy site unless in an unencrypted form.

10. How will computer activity be monitored and managed?

Academy computers have Impero software installed. Impero is a classroom management and computer monitoring software. The software produces reports of inappropriate activity and these reports are collated and dealt with regularly. The software has a number of e-safety features:

- prevent access to unsuitable sites
- prevent unauthorised use of proxy sites
- enforce acceptable usage policy
- create key word libraries for real-time detection
- monitor using specialist built-in key word libraries
- determine potential risk through key word glossaries with explanations
- create different policies depending on severity
- capture time stamped screen shots of every violation
- add screenshots to logviewer report
- record on-screen activity and specify recording length to capture misuse
- export violations with details and image to PDF
- evidence misconduct from a centralised log to support disciplinary action
- alert the relevant authority when rules are violated
- apply policies and filters to laptops when disconnected from the network
- log and monitor all web activity
- enable students to anonymously report concerns using the Confide system.

Policy Decisions

1. How will Internet access be authorised?

The Academy will maintain a current record of all staff and students who are granted access to the Academy's electronic communications.

All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any Academy ICT resource.

Secondary students must apply for Internet access individually by agreeing to comply with the e–Safety Rules.

Parents will be asked to sign and return a consent form for student access.

Staff retain the right to turn Internet use off in a classroom if its use is a distraction to learning following abuse by students.

11. How will risks be assessed?

The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an Academy computer. The Academy can accept liability for the material accessed, or any consequences resulting from Internet use.

The Academy should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

12. How will e–Safety complaints be handled?

Complaints of Internet misuse will be dealt with under the Academy's Complaints Procedure.

Any complaint about staff misuse must be referred to the Principal.

All e–Safety complaints and incidents will be recorded by the Academy — including any actions taken.

Students and parents will be informed of the complaints procedure.

Parents and students will work in partnership with staff to resolve issues.

Discussions will be held with the local Police Safer Academies Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.

Any issues (including sanctions) will be dealt with according to the Academy's disciplinary and child protection procedures.

13. How is the Internet used across the community?
The Academy will liaise with local organisations to establish a common approach to e–Safety.

The Academy will be sensitive to Internet related issues experienced by students out of Academy, e.g. social networking sites, and offer appropriate advice.

14. How will Cyberbullying be managed?
Cyberbullying (along with all forms of bullying) will not be tolerated in Academy. Full details are set out in the Academy's policy on anti-bullying.

There will be clear procedures in place to support anyone affected by Cyberbullying.

All incidents of cyberbullying reported to the Academy will be recorded.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:

Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The Academy will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at Academy for the user for a period of time.
- Parent/carers may be informed.
- Sanctions in line with the Behaviour Policy.
- The Police will be contacted if a criminal offence is suspected.

15. How will Learning Platforms and learning environments be managed?
SLT and staff will monitor the usage of TGi-Space (Learning Platform / Virtual Learning Environment) by students and staff regularly in all areas, in particular message and communication tools and publishing facilities.

Students/staff will be advised on acceptable conduct and use when using the learning platform.

Only members of the current student, parent/carers and staff community will have access to TGi-Space.

All users will be mindful of copyright issues and will only upload appropriate content onto TGi-Space.

When staff, students etc leave the Academy their account or rights to specific Academy areas will be disabled or transferred to their new establishment.

Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to TGi-Space for the user may be suspended.
- Sanctions in line with behaviour policy used.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A student's parent/carer may be informed.
- A visitor (such as an exam moderator) may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Communication Policy

1. How will the policy be introduced to students?

All users will be informed that network and Internet use will be monitored.

An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

Student instruction in responsible and safe use should precede Internet access.

An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe Academy and home use.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable.

A desktop link to the esafety site for the academies will be on each computer.

2. How will the policy be discussed with staff?

The e–Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and students, the Academy will implement Acceptable Use Policies.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct from all staff is essential.

3. How will parents' support be enlisted?

Parents' attention will be drawn to the Academy e–Safety Policy in newsletters, the Academy brochure and on the Academy website.

A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.

Parents will be requested to sign an e–Safety/internet agreement as part of the Home Academy Agreement.

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Interested parents will be referred to organisations listed in section "e–Safety Contacts and References."

Appendix 1: e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre*):* *www.ceop.police.uk*

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

Internet Watch Foundation: *www.iwf.org.uk*

Kidsmart: *www.kidsmart.org.uk*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*

Appendix 2: Staff (and Volunteer) Acceptable Use Policy Agreement

Academy Policy
New technologies have become integral to the lives of children and young people in today's society, both within Academies / academies and in their lives outside Academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy / academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that studentsreceive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Academy ICT systems (eg laptops, email, VLE etc) out of Academy, and to the transfer of personal data (digital or paper based) out of Academy.
- I understand that the Academy ICT systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Academy ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the Academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat or social networking sites.

- I will only communicate with studentsand parents / carers using official Academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Academy have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the Academy / academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant Academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Academy policies.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of Academy ICT equipment in Academy, but also applies to my use of Academy ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Academy ICT systems (both in and out of Academy) and my own devices (in Academy and when carrying out communications related to the Academy) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Appendix 3: Student Acceptable Use Agreement

Academy Policy

Digital technologies 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. These technologies 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.

This Acceptable Use Policy is intended to ensure:

- 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 students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will not bring my own personal devices (mobile phones / tablets / laptops etc) into the Academy unless I have been given permission (only Sixth Form students are given this privilege). I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Appendix 4: Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the academy systems and devices (both in and out of the Academy)
- I not use my own devices in the Academy unless I have been given permission to do so.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy eg communicating with other members of the school, accessing school email, TGi-Space, website etc.

Name of Student	
Group / Class	
Signed	
Date	

Parent / Carer Countersignature

Name of Parent	
Signed	
Date	