Verpflichtung auf das Datengeheimnis sowie zum ordnungsgemäßen Umgang mit der EDV und Daten des SuS - Rhede

des Mitgliedes : (Name-Vorname) _____

(im folgenden Mitglied genannt).

Präambel

Gemäß Art. 24 der Europäischen Datenschutz – Grundverordnung (EU-DSGVO) hat der Verein unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.
Dies vorausgeschickt, werden alle zur Verarbeitung von personenbezogenen Daten befugten Personen in unserem Verein gemäß der nachfolgenden Regelungen zur Vertraulichkeit verpflichtet.

Hiermit erklärt das Mitglied, dass er heute über Geheimhaltungs- und Sorgfaltspflichten im Zusammenhang mit der Bearbeitung von Daten, Projekten und Aufträgen sowie im Umgang mit Informations- und Telekommunikationstechnik und Datenverarbeitungsanlagen des Vereins:

SuS - Rhede

wie nachfolgend angehalten und sodann

1. zur Geheimhaltung aller mit der Tätigkeit zusammenhängenden Informationen,
2. auf das Datengeheimnis (siehe § 1 dieser Verpflichtungserklärung)
3. auf das Fernmeldegeheimnis nach § 88 Telekommunikationsgesetz (TKG) und
4. zum sorgfältigen Umgang mit Informations- und Telekommunikationstechnik und Datenverarbeitungsanlagen

verpflichtet wurde.

§ 1 Datengeheimnis

1. Es ist dem Mitglied untersagt, geschützte personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Nutzen ist jede andere Verwendung personenbezogener Daten (z.B. Veröffentlichung, Datenauswertung und Datenvergleich).

2. Die Einsichtnahme in Logfiles und andere Daten, die personenbezogene Angaben enthalten können, ist nur dann zulässig, wenn dies zur Erfüllung der geschuldeten Tätigkeit oder aus zwingenden technischen Gründen erforderlich ist. Dabei gilt die bloße technische Möglichkeit des Zugriffs auf Daten nicht bereits als Genehmigung, die Daten auch tatsächlich zur Kenntnis nehmen bzw. verarbeiten zu dürfen.

§ 2 Umgang mit Daten

1. Die Verarbeitung der Daten erfolgt grundsätzlich ausschließlich in deren Geschäftsräumen oder vom Vorstand genehmigten Räumen.

2. Die Daten des Vereins dürfen sich nur nach schriftlicher Genehmigung außerhalb der Geschäftsräume befinden, insbesondere in privaten Räumen. Dies gilt unabhängig davon, in welcher Form die Daten vorliegen (elektronisch, als Ausdruck, auf Datenträgern, …).

3. Die Daten sind auch bei der Verarbeitung außerhalb der Geschäftsräume des Vereines sicher gegen unbefugte Kenntnisnahme und Zugriff Dritter zu verwahren.

§ 3 Verschwiegenheitspflichten des Mitgliedes

1. Das Mitglied ist verpflichtet, alle im Rahmen seiner Mitgliedschaft erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Vereines geheim zu halten und auf keinen Fall Dritten zur Kenntnis zu bringen.

2. Diese Verpflichtung besteht auch nach Beendigung des Mitgliedsverhältnisses unbefristet fort.

3. Bei Beendigung des Mitgliedsverhältnisses hat das Mitglied sämtliche in seinem Besitz gelangten Unterlagen und erstellten Verarbeitungs- bzw. Nutzungsergebnisse, die im Zusammenhang mit dem Mitgliedsverhältnis stehen, dem Verein auszuhändigen. Etwaige im Eigentum des Mitglieds befindliche Datenträger mit Daten des Vereines sind nach deren vorheriger Zustimmung physisch zu löschen, soweit eine Rückgabe nicht erforderlich ist.

§ 4 Nutzung der ITK Infrastrukturen (insbesondere: eMail, Internet, Telefon)

1. Die private Nutzung von Hardware und Software aller Internet-Dienstleistungen (wie z.B. WWW, eMail, FTP) in den Räumen des Vereines oder über deren Netzwerke ist dem Mitglied untersagt. Eine Ausnahmeregelung kann nur vom Vorstand getroffen werden.

2. Die illegale Vervielfältigung von Software (Raubkopien) sowie die Weitergabe und die Benutzung derartiger rechtswidrig vervielfältigter Software auf dem System des Vereins sind dem Mitglied untersagt.

3. Zur Eingrenzung der Virengefahr darf das Mitglied nur die vom Verein zur Verfügung gestellte Software verwenden, es sei denn, die berechtigte Stelle des Vereines hat schriftlich zugestimmt (Freigabe).

§ 5 Sorgfältiger Umgang mit ITK- und DV-Anlagen

Nicht ordnungsgemäß erworbene Versionen von Computersoftware können einen Verstoß gegen das Urheberrecht bedeuten und sowohl den Verein als auch das Mitglied, der die Software zum Einsatz bringt, in straf- und zivilrechtliche Haftung bringen. Darüber hinaus besteht die Gefahr, heimliche Schadenssoftware durch illegale Softwarekopien auf betriebliche PCs zu laden oder andere Funktionsstörungen hervorzurufen.

Die Risiken für schwere Schäden aufgrund von Computerviren und anderen schadensstiftenden Programmen erfordern die strikte Beachtung folgender Grundsätze:

1. Die dem Mitglied für seine Tätigkeit zur Verfügung gestellte Software des Vereines ist nur auf der von dem Verein zur Verfügung gestellten Hardware zu betreiben. Das Vervielfältigen von Software (ausgenommen: Sicherungskopie) für den Zweck des Betreibens auf fremder oder anderer eigener Hardware ist nicht gestattet, oder bedarf der schriftlichen Genehmigung des Vorstandes.

2. Es ist untersagt, Spielsoftware, Freeware oder Public Domain Software usw. auf PCs des Vereines zum Einsatz zu bringen, es sei denn, die berechtigte Stelle des Vereines hat schriftlich zugestimmt (Freigabe).

3. Demonstrationssoftware, die auf Anforderung oder unaufgefordert von einem Softwareanbieter zur Verfügung gestellt wird, darf nur in Abstimmung mit der in 2 genannten Stelle getestet werden.

4. Auf privaten PCs erstellte oder kopierte Programme dürfen auf PCs nicht installiert werden.

§ 6 Kontrolle, Sanktionen

1. Der Verein ist befugt, die Einhaltung dieser Vereinbarung durch Stichprobenkontrollen sicherzustellen.

2. Bei Verstößen gegen diese Vereinbarungen sind Schadensersatzansprüche des Vereines gegen das Mitglied möglich sowie Abmahnungen, ordentliche und ggf. außerordentliche Kündigung.

3. Sonstige Geheimhaltungspflichten werden durch diese Verpflichtung nicht berührt.

Mögliche Rechtsfolgen

Verstöße gegen die betrieblichen Geheimhaltungspflichten können zivil- sowie strafrechtlich nach dem Wettbewerbsrecht (UWG) geahndet werden.

Verstöße gegen das Fernmeldegeheimnis können nach § 206 Strafgesetzbuch (StGB) bestraft werden.

Die Verwendung von illegal kopierter Software kann nach dem Urheberrecht strafrechtlich (§ 106 UrhG) und zivilrechtlich verfolgt werden. Die Verbreitung von Schadenssoftware wird gemäß § 303 b StGB strafrechtlich verfolgt.

Im Übrigen sind der unbefugte Abruf geschützter Daten und die Zerstörung von Daten ebenfalls strafbar (§§ 202a, 263a StGB).

Das Mitglied hat diese Vereinbarung zur Kenntnis genommen und eine Kopie dieser Vereinbarung inkl. Anhang zu dieser Vereinbarung ausgehändigt erhalten.

Rhede, den _____

VORNAME NACHNAME

- Vorstand -

VORNAME NACHNAME

Anlage zur Verpflichtungserklärung auf das Datengeheimnis sowie zum ordnungsgemäßen Umgang mit der EDV und Daten des **SuS - Rhede**

Im Folgenden finden Sie eine Auswahl wichtiger Gesetzesstellen, die die Grundlage für die o. g. Verpflichtungserklärung bilden. Diese Aufstellung erhebt keinerlei Anspruch auf Richtigkeit oder Vollständigkeit und dient lediglich zur ersten Information und Orientierung.

Gesetz gegen den unlauteren Wettbewerb (UWG)

UWG 2004 § 17 Verrat von Geschäfts- und Betriebsgeheimnissen

(1) Wer als eine bei einem Verein beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Vereins Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Verein Schaden zuzufügen,

1. sich ein Geschäfts- oder Betriebsgeheimnis durch
   a) Anwendung technischer Mittel,
   b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
   c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,
   unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig handelt,
2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder
3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.

(5) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(6) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

Telekommunikationsgesetz (TKG)

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

Urheberrechtsgesetz (UrhG)

UrhG § 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Strafgesetzbuch (StGB)

StGB § 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

StGB § 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Vereins bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

eine Sendung, die einem solchen Verein zur Übermittlung anvertraut worden und verschlossen ist,
1. öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Verein zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Verein wahrnehmen,
2. von einem solchen Verein oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Vereins dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

StGB § 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

StGB § 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

StGB § 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.